UNIVERSITY OF ILLINOIS
GRADUATE COLLEGE
DIGITAL COMPUTER LABORATORY

REPORT NO. 78

A THEORY OF ASYNCHRONOUS CIRCUITS II

D. E. Muller and W. Scott Bartky

March 13, 1957

This work has been supported in part by
the Office of Naval Research under
Contract NR 044 001

6. Length of an $\mathcal{R}$-Sequence

6.1 Partial allowed sequences in circuits which are semi-modular with respect to an initial state u (such a circuit will be abbreviated sm[u]) exhibit important length properties. In order to study these properties, however, it is convenient to treat a somewhat more general sequence, called an $\mathcal{R}$-sequence.

(6:1) An $\mathcal{R}$-sequence a(1), a(2), ..., a(k) is any finite sequence of states in which a(i) $\mathcal{R}$ a(i+1) for all i = 1, 2, ..., k-1.

We note that this definition is more general than the definition of a partial allowed sequence (3:2) since the restriction a(i) $\neq$ a(i+1) has been removed. Therefore, any partial allowed sequence is an $\mathcal{R}$-sequence. Also, for any $\mathcal{R}$-sequence we can find a corresponding partial allowed sequence if sub-sequences consisting of equal states are replaced by single states.

(6:2) In an $\mathcal{R}$-sequence a(1), a(2), ..., a(k) we say that a consecutive pair of states a(i), a(i+1) is redundant if and only if a(i) = a(i+1).

Thus, a partial allowed sequence is an $\mathcal{R}$-sequence having no redundant pairs.

(6:3) Given any $\mathcal{R}$-sequence a(1), a(2), ..., a(k) we define an n-dimensional "length" vector L[a(1), a(2), ..., a(k)] recursively by:

(6:3a) $L[a(1)] = (0, 0, \ldots, 0)$

(6:3b) $L[a(i), a(i+1)] = (\ell_1, \ell_2, \ldots, \ell_n)$, where $\ell_j = |a_j(i+1) - a_j(i)|$

(6:3c) $L[a(1), a(2), \ldots, a(i+1)] = L[a(1), a(2), \ldots, a(i)] + L[a(i), a(i+1)]$.

Componentwise vector addition is assumed in (6:3c). One may interpret the i'th component of L[a(1), a(2), ..., a(k)] as the sum of the magnitudes of the changes that have occurred in the i'th signal while passing through the $\mathcal{R}$-sequence a(1), a(2), ..., a(k).

6.2 In the succeeding sections the following vector operations will be needed:

(6:4) $L[a(1), a(2), \ldots, a(k)] \leq L[b(1), b(2), \ldots, b(t)]$ means each component of $L[a(1), a(2), \ldots, a(k)]$ is less than or equal to the corresponding component of $L[b(1), b(2), \ldots, b(t)]$.

(6:5) $L[a(1), a(2), \ldots, a(k)] \vee L[b(1), b(2), \ldots, b(t)]$ is a vector whose components are the pairwise maxima of the corresponding components of $L[a(1), a(2), \ldots, a(k)]$ and $L[b(1), b(2), \ldots, b(t)]$.

(6:6) $L[a(1), a(2), \ldots, a(k)] \wedge L[b(1), b(2), \ldots, b(t)]$ is a vector whose components are the pairwise minima of the corresponding components of $L[a(1), a(2), \ldots, a(k)]$ and $L[b(1), b(2), \ldots, b(t)]$.

Several properties of such vectors may be readily verified. They are:

(6:7) $L[a(1), a(2), \ldots, a(j), \ldots, a(k)] = L[a(1), a(2), \ldots, a(j)] + L[a(j), a(j+1), \ldots, a(k)]$.

(6:8) $L[a(1), a(2), \ldots, a(j)] \leq L[a(1), a(2), \ldots, a(k)]$ whenever $j \leq k$.

(6:9) $L[a(1), a(2), \ldots, a(k)] = 0$ if and only if $a(j) = a(1)$ for all $j = 1, 2, \ldots, k$.

As a consequence of (6:7) and (6:9) the length of an $\mathcal{R}$-sequence is unchanged if it is contracted to form a partial allowed sequence as described in paragraph 6.1.

6.3 Some properties of the state $M[a; b, c]$ were developed in 5.4. Further properties concerned with length vectors may now be described.

(6:10) In an sm[u] circuit let $u \mathcal{F} a$, $a \mathcal{R} b$, and $a \mathcal{R} c$. If we write $d = M[a; b, c]$, then $L[a, d] = L[a, b, d] = L[a, c, d] = L[a, b] \vee L[a, c]$.

<u>Proof</u>: By (5:5) $a \mathcal{R} d$, $b \mathcal{R} d$, and $c \mathcal{R} d$ so that the expressions $L[a, d]$, $L[a, b, d]$, and $L[a, c, d]$ may be written. Now by the definition of $M[a; b, c]$ given in (5:4) if $a_i \leq a_i'$ we have either $a_i \leq b_i \leq c_i = d_i$ or $a_i \leq c_i \leq b_i = d_i$ or both. In either case

(6:11) $|d_i - a_i| = |d_i - b_i| + |b_i - a_i| = |d_i - c_i| + |c_i - a_i| = \text{Max.}\ [|b_i - a_i|, |c_i - a_i|]$.

Similarly if $a_i \geq a_i'$ we have either $a_i \geq b_i \geq c_i = d_i$ or $a_i \geq c_i \geq b_i = d_i$ or both and (6:11) still holds.

6.4 Since any $\mathcal{R}$-sequence can be contracted to a partial allowed sequence we note that if $u \mathfrak{J} a(1)$ and if a(1), a(2), ..., a(k) is an $\mathcal{R}$-sequence then $u \mathfrak{J} a(i)$ for all i = 1, 2, ..., k. We may therefore extend (5:6) to yield.

(6:12) Let $u \mathfrak{J} a(1, 1)$ in an sm[u] circuit and let a(1, 1), a(1, 2), ..., a(1, j) and a(1, 1), a(2, 1), ..., a(i, 1) be two $\mathcal{R}$-sequences. We may then define a(r, s) = M[a(r-1, s-1); a(r-1, s), a(r, s-1)] recursively for r = 2, 3, ..., i and s = 2, 3, ..., j.

The results given in (6:10) and (6:12) may now be used to generalize (6:10) to:

(6:A) Under the assumptions of (6:12)

(6:13) $L[a(1, 1), a(1, 2), \ldots, a(1, j), a(2, j) \ldots, a(i, j)]$

$= L[a(1, 1), a(2, 1), \ldots, a(i, 1), a(i, 2), \ldots, a(i, j)]$

$= L[a(1, 1), a(1, 2), \ldots, a(1, j)] \vee L[a(1, 1), a(2, 1), \ldots, a(i, 1)].$

Proof: Equations (6:13) hold trivially when either i = 1 or j = 1. Let us assume (6:13) holds if indices (i, j) are replaced by (i-1, j-1), (i-1, j) or (i, j-1) and prove the result by induction. By (6:10) we have:

(6:14) $L[a(i-1, j-1), a(i, j-1), a(i, j)] = L[a(i-1, j-1), a(i-1, j), a(i, j)]$

$= L[a(i-1, j-1), a(i, j-1)] \vee L[a(i-1, j-1), a(i-1, j)].$

We have assumed

(6:15) $L[a(1, 1), a(1, 2), \ldots, a(1, j-1), a(2, j-1), \ldots, a(i-1, j-1)]$

$= L[a(1, 1), a(2, 1), \ldots, a(i-1, 1), a(i-1, 2), \ldots, a(i-1, j-1)].$

Use is now made of the following property of numerical vectors.

(6:16) If w, x, y, and z are numerical vectors and $x \vee y = z$, then $(x + w) \vee (y + w) = z + w$.

Using properties (6:16) and (6:7) we suitably add terms of (6:15) to (6:14) and obtain:

$$(6{:}17)\quad L[a(1, 1), a(1, 2), \ldots, a(1, j-1), a(2, j-1), \ldots, a(i, j-1)]$$
$$+ L[a(i, j-1), a(i, j)]$$
$$= L[a(1, 1), a(2, 1), \ldots, a(i-1, 1), a(i-1, 2), \ldots, a(i-1, j)]$$
$$+ L[a(i-1, j), a(i, j)]$$
$$= L[a(1, 1), a(1, 2), \ldots, a(1, j-1), a(2, j-1), \ldots, a(i, j-1)] \vee$$
$$L[a(1, 1), a(2, 1), \ldots, a(i-1, 1), a(i-1, 2), \ldots, a(i-1, j)].$$

But by the induction hypothesis on (i, j-1) we have

$$(6{:}18)\quad L[a(1, 1), a(1, 2), \ldots, a(1, j-1), a(2, j-1), \ldots, a(i, j-1)]$$
$$= L[a(1, 1), a(2, 1), \ldots, a(i, 1), a(i, 2), \ldots, a(i, j-1)]$$
$$= L[a(1, 1), a(1, 2), \ldots, a(i, j-1)] \vee L[a(1, 1), a(2, 1), \ldots, a(i, 1)]$$

and on (i-1, j)

$$(6{:}19)\quad L[a(1, 1), a(1, 2), \ldots, a(1, j), a(2, j), \ldots, a(i-1, j)]$$
$$= L[a(1, 1), a(2, 1), \ldots, a(i-1, 1), a(i-1, 2), \ldots, a(i-1, j)]$$
$$= L[a(1, 1), a(1, 2), \ldots, a(1, j)] \vee L[a(1, 1), a(2, 1), \ldots, a(i-1, 1)].$$

Substituting (6:18) and (6:19) in (6:17) we obtain:

$$(6{:}20)\quad L[a(1, 1), a(2, 1) \ldots, a(i, 1), a(i, 2), \ldots, a(i, j-1)]$$
$$+ L[a(i, j-1), a(i, j)]$$
$$= L[a(1, 1), a(1, 2), \ldots, a(i, j), a(2, j), \ldots, a(i-1, j)]$$
$$+ L[a(i-1, j), a(i, j)] = L[a(1, 1), a(1, 2), \ldots, a(1, j-1)] \vee$$
$$L[a(1,1), a(2, 1), \ldots, a(i, 1)] \vee L[a(1, 1), a(1, 2), \ldots, a(1, j)] \vee$$
$$L[a(1, 1), a(2, 1), \ldots, a(i-1, 1)].$$

In this expression we make use of a further property of numerical vectors.

(6:21) If x and y are numerical vectors and if $x \leq y$ then $x \vee y = y$.

The 1st and 4th in the last expression of (6:20) are less than the 3rd and 2nd terms respectively so that (6:20) may be reduced to (6:13) by use of (6:7) and (6:8). Thus, by induction (6:13) holds for all i and j, and (6:A) is proved.

7. Cummulative States

7.1 The result contained in (6:A) may be used to simplify the theory of semi-modular circuits and express it in a new form which permits many of the properties of such circuits to be easily demonstrated. This reformulation involves introducing the notion of a cummulative state (to be abbreviated C-state) which not only determines the state of the circuit but also the important features of the partial allowed sequence through which the circuit passed in reaching this state.

(7:1) A cummulative state (or C-state) $\underline{a}$ of a partial allowed sequence u, a(1), a(2), ..., a(k), a in an sm[u] circuit is defined as L[u, a(1), a(2), ..., a(k), a].

A C-state, thus, is an n-dimensional vector having non-negative integral components since it is equal to the length of a partial allowed sequence. Although a partial allowed sequence whose length is $\underline{a}$ must exist in order to define the C-state $\underline{a}$, we note that more than one such sequence may exist, as was demonstrated in (6:10). The state u in (7:1) is called the initial state and a the terminal state corresponding to $\underline{a}$ and its partial allowed sequence.

(7:A) In an sm[u] circuit if $\underline{a}$ is a C-state having initial state u, then the terminal state of $\underline{a}$ is uniquely determined independently of which partial allowed sequence is used to define $\underline{a}$.

Proof: This result is proved trivially in the binary case, because the components of $\underline{a}$ are simply the numbers of changes which have occurred in the signals while passing from u to the terminal state. Thus the respective signals of this terminal state will either agree of disagree with those of u depending upon whether an even or an odd number of changes have occurred and consequently upon whether the corresponding components of $\underline{a}$ are even or odd.

In the general case we must use (6:A) to prove uniqueness. Let us assume two partial allowed sequences correspond to $\underline{a}$ so that

$$\underline{a} = L[u, a(1, 2), a(1, 3), \ldots, a(1, j)]$$
$$= L[u, a(2, 1), a(3, 1), \ldots, a(i, 1)].$$

Then by (6:A) we may form $\mathcal{R}$-sequences such that

$L[u, a(1, 2), a(1, 3), \ldots, a(1, j), a(2, j), \ldots, a(i, j)]$

$= L[u, a(1, 2), a(1, 3), \ldots, a(1, j)] \vee$

$L[u, a(2, 1), a(3, 1), \ldots, a(i, 1)] = \underline{a} \vee \underline{a} = \underline{a}$. Thus we have

$\underline{a} + L[a(1, j), a(2, j), \ldots, a(i, j)] = \underline{a}$; hence

$L[a(1, j), a(2, j), \ldots, a(i, j)] = 0$ by (6:7), and (6:9) yields

$a(1, j) = a(i, j)$.

A similar argument gives us $a(j, 1) = a(i, j)$ and the two terminal states are identical.

Since the terminal state is determined by the C-state (and the initial state u) we shall use the notation $t(\underline{a})$ to represent the terminal state corresponding to $\underline{a}$ or, when convenient, use the same letter designation (in this case $a = t(\underline{a})$) for it.

7.2 Of particular interest are the relationships between the C-states which have a particular state u as their initial state. The set of such C-states (which may be infinite) will be called C[u]. Such a set of C-states will be shown to form a semi-modular lattice under a suitable ordering. It is for this reason that we have used the term semi-modular in the description of circuits.

The set C[u] will be used to display the properties of semi-modular circuits more easily and completely than is possible merely using the notion of allowed sequences.

We begin by defining the $\mathfrak{J}$ relationship with respect to C-states.

(7:2) If $\underline{a}$ and $\underline{b}$ are in C[u] with terminal states a and b respectively, we define $\underline{a} \mathfrak{J} \underline{b}$ to mean that there exists a partial allowed sequence $a, a(1), a(2), \ldots, a(k), b$ such that $L[a, a(1), a(2), \ldots, a(k), b] + \underline{a} = \underline{b}$.

Using this definition and (7:1) we may restate (6:A) as follows:

(7:3) If $\underline{a}$ and $\underline{b}$ are in C[u] then $\underline{c} = \underline{a} \vee \underline{b}$ is in C[u] and $\underline{a}\,\mathfrak{J}\,\underline{c}$ and $\underline{b}\,\mathfrak{J}\,\underline{c}$.

This theorem in the form given above is now used to show that C[u] is a lattice under the $\mathfrak{J}$ relationship.

(7:4) Given $\underline{a}$ and $\underline{b}$ in C[u] then $\underline{a}\,\mathfrak{J}\,\underline{b}$ if and only if $\underline{a} \leq \underline{b}$.

<u>Proof</u>: Assume $\underline{a}\,\mathfrak{J}\,\underline{b}$ so that by (7:2) there is a partial allowed sequence a, a(1), a(2), ..., a(k), b such that $L[a, a(1), a(2), \ldots, a(k), b] + \underline{a} = \underline{b}$. Since the length vector has non-negative components we have $\underline{a} \leq \underline{b}$.

Assume $\underline{a} \leq \underline{b}$. Then $\underline{a} \vee \underline{b} = \underline{b}$ and by (7:3) $\underline{a}\,\mathfrak{J}\,\underline{a} \vee \underline{b} = \underline{b}$, and the theorem is proved.

We see from (7:4) that the elements of C[u] are partially ordered under the relationship since it is equivalent to the ($\leq$) relationship of numerical vectors which defines a partial ordering.

By combining (7:3) and (7:4) we may extend (6:A) further, to another form. This form of (6:A), given in (7:5) provides a simpler and more natural way of stating this basic concept.

(7:5) If $\underline{a}$ and $\underline{b}$ are in C[u] then $\underline{a} \vee \underline{b}$ is in C[u] and is their least upper bound under the $\mathfrak{J}$ relationship.

<u>Proof</u>: That $\underline{a} \vee \underline{b}$ is an upper bound in C[u] follows from (7:3). It is also a least upper bound since it is a numerical least upper bound, and by (7:4) this is equivalent to its being a least upper bound under the $\mathfrak{J}$ relationship. Hence, we shall use the notation $\underline{a} \cup \underline{b}$ (the least upper bound of $\underline{a}$ and $\underline{b}$) interchangeably with $\underline{a} \vee \underline{b}$.

(7:6) If $\underline{a}$ and $\underline{b}$ are in C[u] then their greatest lower bound (written $\underline{a} \cap \underline{b}$) in C[u] exists.

<u>Proof</u>: The set of all C-states $\underline{m}$ such that $\underline{m}\,\mathfrak{J}\,\underline{a}$ and $\underline{m}\,\mathfrak{J}\,\underline{b}$ is finite since all such $\underline{m}$ must have non-negative integral components which are all less than or equal to the corresponding components of $\underline{a}$. Let us designate these C-states as

$\underline{m}(1), \underline{m}(2), \ldots, \underline{m}(j)$. This set is non-empty since we may form a C-state $\underline{0}$, whose components are all zero from the partial allowed sequence consisting only of the initial state u. By (7:4) $\underline{0} \mathfrak{J} \underline{x}$ for all $\underline{x}$ in C[u] and, therefore, is a lower bound of $\underline{a}$ and $\underline{b}$. Now form $\underline{m}(1) \cup \underline{m}(2) \cup \ldots \cup \underline{m}(j) = \underline{c}$. By (7:5) we have $\underline{c} \mathfrak{J} \underline{a}$ and $\underline{c} \mathfrak{J} \underline{b}$ and yet $\underline{m}(i) \mathfrak{J} \underline{c}$ for all $\underline{m}(i)$. Hence $\underline{c} = \underline{a} \cap \underline{b}$.

Combining the results (7:4), (7:5), and (7:6) and the discussion of $\underline{0}$ in the proof of (7:6) we have:

(7:B) C[u] is a lattice with a zero under the partial ordering relationship $\mathfrak{J}$.

It should be observed at this point that $\underline{a} \cap \underline{b}$, while the greatest lower bound of $\underline{a}$ and $\underline{b}$ in C[u], is not necessarily the numerical intersection $\underline{a} \wedge \underline{b}$. This latter vector may not be a C-state in C[u] although, if it is, then the two intersections are equal by (7:4).

7.3 We now wish to show that the lattice of (7:B) is a semimodular lattice. This is done most easily by introducing an $\mathcal{R}$ relationship among the C-states in C[u].

(7:7) $\underline{a} \mathcal{R} \underline{b}$ means $a \mathcal{R} b$ and $\underline{b} = L[a, b] + \underline{a}$

Here it is understood that $a = t(\underline{a})$ and $b = t(\underline{b})$. By (7:1), we note that if $\underline{a}$ is in C[u] and $a \mathcal{R} b$ we may always form $\underline{b}$ in C[u] so that $\underline{a} \mathcal{R} \underline{b}$. Thus we may go on to define

(7:8) $\underline{a}' = L[a, a'] + \underline{a}$

for any $\underline{a}$ in C[u] since $a \mathcal{R} a'$ by (3:1). By (7:7) we see that $\underline{a} \mathcal{R} \underline{a}'$ for all $\underline{a}$. Using these definitions we may parallel some of the results in sections 3 and 5, with the C-states in C[u] replacing the states of S. The following theorem is analogous to (3:1)

(7:9) $\underline{a} \mathcal{R} \underline{b}$ if and only if $\underline{a} \leq \underline{b} \leq \underline{a}'$

By (7:4) this second condition is equivalent to $\underline{a} \mathfrak{J} \underline{b} \mathfrak{J} \underline{a}'$.

Proof of (7:9): If $\underline{a}\mathcal{R}\underline{b}$ we have $a\mathcal{R}b$ so that for each signal we have either $a_i \leq b_i \leq a_i'$ or $a_i \geq b_i \geq a_i'$ and in either case $|b_i - a_i| \leq |a_i' - a_i|$ but since $a\mathcal{R}b$ and $a\mathcal{R}a'$ this implies $|b_i - a_i| = \underline{b}_i - \underline{a}_i$ and $|a_i - a_i'| = \underline{a}_i - \underline{a}_i'$, where $\underline{a}_i$, $\underline{b}_i$ and $\underline{a}_i'$ are the i'th components of $\underline{a}$, $\underline{b}$, and $\underline{a}'$. Thus $\underline{b} \leq \underline{a}'$ and since $|b_i - a_i| \geq 0$ we have $\underline{a} \leq \underline{b}$.

Assume next that $\underline{a} \leq \underline{b} \leq \underline{a}'$. Construct a state b^* as follows: Let $b_i^* = a_i + (\underline{b}_i - \underline{a}_i)$ if $a_i \leq a_i'$ and let $b_i^* = a_i - (\underline{b}_i - \underline{a}_i)$ if $a_i > a_i'$. Then since $|a_i' - a_i| = \underline{a}_i' - \underline{a}_i$ we have $a_i \leq b_i^* \leq a_i'$ if $a_i \leq a_i'$, and $a_i \geq b_i^* \geq a_i'$ if $a_i > a_i'$. Hence $a\mathcal{R}b^*$. But $b^* = b$ since $L[a, b^*] = \underline{b} - \underline{a}$, and (7:7) is therefore satisfied.

(7:10) If $\underline{a}\mathcal{R}\underline{b}$ then $\underline{b}\mathcal{R}\underline{a}'$.

Proof: This result is analogous to (5:3). From (5:3) we have $b\mathcal{R}a'$. We need only show that $L[b, a'] + \underline{b} = \underline{a}'$. Since $|a_i' - b_i| + |b_i - a_i| = |a_i' - a_i|$ by (3:1), we have $L[a, b] + L[b, a'] = L[a, a']$ and $L[b, a'] = L[a, a'] - L[a, b]$ $= (\underline{a}' - \underline{a}) - (\underline{b} - \underline{a}) = \underline{a}' - \underline{b}$.

(7:11) If $\underline{a}\mathcal{R}\underline{c}$ and $\underline{a} \leq \underline{b} \leq \underline{c}$ then $\underline{a}\mathcal{R}\underline{b}\mathcal{R}\underline{c}$.

Proof: By (7:9) $\underline{c} \leq \underline{a}'$ so $\underline{a} \leq \underline{b} \leq \underline{a}'$ and hence $\underline{a}\mathcal{R}\underline{b}$. Also by (7:10) $\underline{b}\mathcal{R}\underline{a}'$ so $\underline{a}' \leq \underline{b}'$ and hence $\underline{b} \leq \underline{c} \leq \underline{a}' \leq \underline{b}'$ and $\underline{b}\mathcal{R}\underline{c}$.

(7:12) If $\underline{a}\mathcal{R}\underline{b}$ and $\underline{a}\mathcal{R}\underline{c}$ then $\underline{a}\mathcal{R}(\underline{b} \cup \underline{c})$.

Proof: Since $\underline{a} \leq \underline{b} \leq \underline{a}'$ and $\underline{a} \leq \underline{c} \leq \underline{a}'$ we have $\underline{a} \leq \underline{b} \cup \underline{c} \leq \underline{a}'$; hence $\underline{a}\mathcal{R}(\underline{b} \cup \underline{c})$ by (7:9).

(7:13) If $\underline{a}\mathcal{R}\underline{b}$ and $\underline{a}\mathcal{R}\underline{c}$ then $\underline{b} \cap \underline{c} = \underline{b} \wedge \underline{c}$.

Proof: While (7:10) - (7:12) are analogous to properties of the states of S which were given in sections 3 and 5, the result (7:13) is not. Since $a\mathcal{R}b$ and $a\mathcal{R}c$ we may define a state d as follows:

$$d_i = \text{Min}\,[b_i, c_i] \qquad \text{if } a_i \leq a_i'$$

$$d_i = \text{Max}\,[b_i, c_i] \qquad \text{if } a_i \geq a_i'$$

Since b_i and c_i both satisfy the conditions of (3:1) we see that d_i does too and $a \mathcal{R} d$. Also $|d_i - a_i| = \mathrm{Min}\,[|b_i - a_i|, |c_i - a_i|]$ so $L[a, d] = L[a, b] \wedge L[a, c]$ and if we let $\underline{d} = \underline{a} + L[a, d]$ then by (6:16) $\underline{d} = \underline{b} \wedge \underline{c}$. Thus $\underline{b} \wedge \underline{c}$ is in C[u] and since it is a numerical greatest lower bound we see that $\underline{b} \cap \underline{c} = \underline{b} \wedge \underline{c}$. It is now possible to prove

(7:C) The lattice C[u] is semi-modular.

<u>Proof</u>: A lattice is said to be semi-modular if the following condition is satisfied.

(7:14) If $\underline{x}$, $\underline{y}$, and $\underline{a}$ are three elements such that $\underline{x}$ and $\underline{y}$ cover $\underline{a}$ and $\underline{x} \neq \underline{y}$, then $\underline{x} \cup \underline{y}$ covers $\underline{x}$ and $\underline{y}$. (See Ref. 3 page 100.)

In the present lattice C[u] we express the "covers" relationship as follows:

(7:15) If $\underline{r}$ and $\underline{s}$ are in C[u], then $\underline{s}$ covers $\underline{r}$ if and only if $\underline{r} \mathfrak{Z} \underline{s}$, $\underline{r} \neq \underline{s}$ and $\underline{r} \mathfrak{Z} \underline{t} \mathfrak{Z} \underline{s}$ implies either $\underline{r} = \underline{t}$ or $\underline{t} = \underline{s}$. (See Ref. 3, page 5.)

We now seek to prove (7:14). First we show that $\underline{x}$ covers $\underline{a}$ implies $\underline{a} \mathcal{R} \underline{x}$. Since $\underline{a} \mathfrak{Z} \underline{x}$ there is a partial allowed sequence from a to x such that $L[a, a(1), \ldots, a(k), x] = \underline{x} - \underline{a}$. But this implies that $\underline{a}(1) = \underline{a} + L[a, a(1)]$ is such that $\underline{a} \mathcal{R} \underline{a}(1) \mathfrak{Z} \underline{x}$, and by (7:15) this means that $\underline{a}(1) = \underline{x}$ so that the partial allowed sequence contains only two members a, and x. Hence $\underline{a} \mathcal{R} \underline{x}$. Similarly $\underline{a} \mathcal{R} \underline{y}$ and by (7:12) $\underline{a} \mathcal{R} \underline{x} \cup \underline{y}$.

Secondly, we show that $\underline{x} \cup \underline{y}$ covers $\underline{x}$. Let $\underline{b}$ be any C-state such that $\underline{x} \mathfrak{Z} \underline{b} \mathfrak{Z} \underline{x} \cup \underline{y}$. Now by (7:11) we have $a \mathcal{R} b$ and by (7:13) $\underline{y} \cap \underline{b} = \underline{y} \wedge \underline{b}$. Using the distributive properties of numerical vectors $\underline{x} \vee (\underline{y} \wedge \underline{b}) = (\underline{x} \vee \underline{y}) \wedge (\underline{x} \vee \underline{b})$ $= (\underline{x} \vee \underline{y}) \wedge \underline{b} = \underline{b}$. Since $\underline{a} \mathfrak{Z} \underline{y} \wedge \underline{b} \mathfrak{Z} \underline{y}$, by (7:15), either $\underline{y} \wedge \underline{b} = \underline{a}$ or $\underline{y} \wedge \underline{b} = \underline{y}$, so in the former case $\underline{x} = \underline{x} \vee \underline{a} = \underline{x} \vee (\underline{y} \wedge \underline{b}) = \underline{b}$, and in the latter $\underline{x} \vee \underline{y} = \underline{x} \vee (\underline{y} \wedge \underline{b}) = \underline{b}$. Hence $\underline{x} \vee \underline{y}$ covers $\underline{x}$ by (7:15) and similarly $\underline{x} \vee \underline{y}$ covers $\underline{y}$.

7.4 An alternative proof of (7:C) may be obtained if a closer investigation is made into the nature of the "covers" relation.

(7:D) $\underline{b}$ covers $\underline{a}$ if and only if there is one component index i such that $\underline{b}_i = \underline{a}_i + 1$ and $\underline{b}_j = \underline{a}_j$ whenever $j \neq i$.

<u>Proof</u>: If $\underline{b}_i = \underline{a}_i + 1$ and $\underline{b}_j = \underline{a}_j$ whenever $j \neq i$ then $\underline{a} \mathfrak{Z} \underline{b}$ by (7:4) and since the C-states must have integral components (7:15) is satisfied so that $\underline{b}$ covers $\underline{a}$.

If, on the other hand, $\underline{b}$ covers $\underline{a}$, then by the proof of (7:B) $\underline{a} \mathcal{R} \underline{b}$ and $a \mathcal{R} b$. Since $\underline{a} \neq \underline{b}$ there must be some signal index i such that $\underline{a}_i < \underline{b}_i$. Thus $\underline{b}_i - \underline{a}_i = |b_i - a_i| > 0$, and either $a_i < b_i \leq a_i'$ or $a_i > b_i \geq a_i'$. Define a state b* in S by letting $b_j{*} = a_j$ for $j \neq i$ and $b_i{*} = a_i + 1$ if $a_i < a_i'$ but $b_i{*} = a_i - 1$ if $a_i > a_i'$. To show that b* is in S we note that $b_j{*}$ is in S_j since a_j is in S_j and $b_i{*}$ is in S_i, since either $a_i < b_i{*} \leq a_i'$ or $a_i > b_i \geq a_i'$ and both a_i and a_i' are in S_i. Thus we may write $a \mathcal{R} b{*}$ and if we let $\underline{b}{*} = \underline{a} + L[a, b{*}]$ then $\underline{a} \mathcal{R} \underline{b}{*}$. But $\underline{b}{*} \leq \underline{b}$ so $\underline{a} \mathfrak{Z} \underline{b}{*} \mathfrak{Z} \underline{b}$ and since $\underline{a} \neq \underline{b}$ we must have $\underline{b}{*} = \underline{b}$ by (7:15). However, $\underline{b}{*}$ has the properties required of $\underline{b}$ in (7:D).

The proof of (7:D) is unique in that it requires the construction of a state b* in S and thus makes use of the assumption (2:1b) that S is the set of all n-tuples of signals taken from the sets S_i. It is true that constructions have been used before; specifically they have been used in (5:4) and (7:13). In these two constructions somewhat weaker assumptions were involved as we shall see.

In the original choice of signals (2:1a) and functions (2:1c) the assumption (2:1b) amounts to assuming that these signals are independent of each other, so that not only do they describe the state of the circuit, but also that this description is not redundant. This puts the burden on the circuit designer to make certain that the signals he uses to describe the circuit are independent in the sense that he is not using two or more signals to measure some quantity which could be measured by one signal. If two signals were not independent in this sense, the effect would be to make the value of one signal uniquely dependent upon the value

of the other, and the states of S would be correspondingly limited. Now in the constructions of (5:4) and (7:13) such dependence between signals is not violated, while in (7:D) it is. Thus the assumption of independence of the signals has not been used except in the proof of (7:D).

A further assumption is also involved in (7:D) which is not used elsewhere. That is that all the signal levels z_i in the sets S_i may actually occur. This means that the designer must be sure that the k_i signal levels in each set S_i are realizable in the actual circuit. In (5:4) and (7:13) only signal levels in existing states are used in the construction of new states, while in (7:D) a new signal level may be introduced.

Thus we see that new assumptions which were not used in the proofs of previous results occur in the proof of (7:D). It is for this reason that the proof of (7:C) was made independently of (7:D). A simpler proof that C[u] is semi-modular may be obtained if we use (7:D).

Alternative proof of (7:C): We wish to show that if $\underline{x}$ and $\underline{y}$ cover $\underline{a}$ then, $\underline{x} \cup \underline{y}$ covers $\underline{x}$ and $\underline{y}$. By (7:D) there are two signal indices i and j such that $\underline{x}_i = \underline{a}_i + 1$ and $\underline{x}_k = \underline{a}_k$ if $k \neq i$ and $\underline{y}_j = \underline{a}_j + 1$ and $\underline{y}_k = \underline{a}_k$ if $k \neq j$. We see that $i \neq j$, since in the hypothesis of (7:C) $\underline{x} \neq \underline{y}$. Thus if $\underline{x} \cup \underline{y} = \underline{b}$, we have $\underline{b}_i = \underline{a}_i + 1$ and $\underline{b}_j = \underline{a}_j + 1$, $\underline{b}_k = \underline{a}_k$ if $k \neq i$ and $k \neq j$. Therefore by (7:D) $\underline{b}$ covers $\underline{x}$ and $\underline{y}$.

Another theorem that involves the construction of a state, and will be needed later on, is the following:

(7:E) Let $\underline{a}$ be a C-state in C[u] for which $\underline{a}_i \neq \underline{a}_i'$. Then there exists a C-state $\underline{b}$ in C[u] such that $\underline{b}_j = \underline{a}_j$ for $j \neq i$ and $\underline{b}_i = \underline{a}_i + 1$.

<u>Proof</u>: Let a be the terminal state of $\underline{a}$. Since $a_i \neq \underline{a}_i'$ then either $a_i < a_i'$ or $a_i > a_i'$. In the former case define the state b by $b_j = a_j$ for $j \neq i$ and $b_i = a_i + 1$. Then b is a state in S since $a \mathcal{R} b$, and the C-state $\underline{b} = \underline{a} + L[a, b]$

satisfies the theorem. If on the otherhand, $a_j > a_i'$, then the state b would be defined as $b_j = a_j$ for $j \neq i$ and $b_i = a_i - 1$.

We note that under the hypothesis of (7:E), b covers a as a consequence of theorem (7:D).

7.5 To illustrate the relationship between states and C-states, consider the example of the following binary circuit.

$$z_1' = z_2 z_3 \vee z_1 z_2 \vee z_1 z_3 \tag{7:16}$$

$$z_2' = \bar{z}_1$$

$$z_3' = \bar{z}_1$$

This circuit, if represented by a logical diagram, would consist of two "not" elements and a special element "C" for producing the function $z_2 z_3 \vee z_1 z_2 \vee z_1 z_3$. This element has the property that its output z_1 tends to agree with the two inputs z_2 and z_3 if they agree with each other, but it retains its old value if they disagree. This circuit is illustrated in Figure 2.

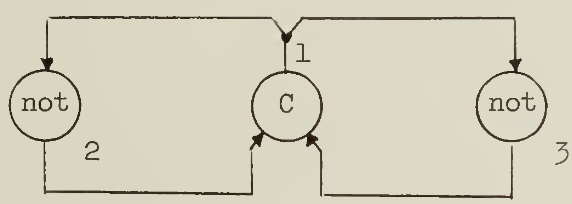

Figure 2

Let us assume that the circuit is placed in the state (0, 1, 1). It must then pass to the state (1, 1, 1). This state may lead to either of the states (1, 0, 1) or (1, 1, 0). Whichever of these occurs, the circuit will then pass to (1, 0, 0) and then to (0, 0, 0). This state may change so as to become either (0, 1, 0) or (0, 0, 1), but either of these leads back to the initial state (0, 1, 1). We may check that (5:3) is satisfied in each transition but not (5:2) so the circuit is semi-modular but not totally sequential. Since the circuit never reaches equilibrium, its lattice C[u] of C-states is infinite. This lattice

is partly illustrated in Figure 3 when $u = (0, 1, 1)$.

$$\begin{tikzcd}
 & (0, 0, 0) \arrow[d] & \\
 & (1, 0, 0) \arrow[dl] \arrow[dr] & \\
(1, 1, 0) \arrow[dr] & & (1, 0, 1) \arrow[dl] \\
 & (1, 1, 1) \arrow[d] & \\
 & (2, 1, 1) \arrow[dl] \arrow[dr] & \\
(2, 2, 1) \arrow[dr] & & (2, 1, 2) \arrow[dl] \\
 & (2, 2, 2) \arrow[d] & \\
 & (3, 2, 2) \arrow[dl] \arrow[dr] & \\
(3, 3, 2) \arrow[dr] & & (3, 2, 3) \arrow[dl] \\
 & {} &
\end{tikzcd}$$

Figure 3

In figure 3 the terminal state corresponding to any C-state may be obtained by adding $u = (0, 1, 1)$ to the C-state and taking residues of each component modulo 2.

8. Cycling Theory

8.1 It was observed in (3.7) that it is possible for a state to recur in a partial allowed sequence. Since the behavior of the circuit depends only on the state, we should expect a repetitive behavior when states may recur. In the present section we shall study this repetitive behavior when it occurs in semi-modular circuits.

(8:1) Let $\underline{v}$ be in $C[u]$ then define

(8:1a) $D[\underline{v}]$ as the set of all C-states $\underline{a}$ in $C[u]$ such that $\underline{v} \mathfrak{J} \underline{a}$ and

(8:1b) $E[\underline{v}]$ as the set of all C-states $\underline{a}$ in $D[\underline{v}]$ such that $t[\underline{v}] = t[\underline{a}]$.

We note that $E[\underline{v}]$ contains only $\underline{v}$ unless the state $t(\underline{v})$ may recur. Also it is easily verified that $D[\underline{v}]$ is a sublattice of $C[u]$.

(8:A) If $\underline{v}$ is in $C[u]$ then the lattice $C[v]$ and the sublattice $D[\underline{v}]$ are isomorphic under the transformation $\underline{a}^* = \underline{v} + \underline{a}$, where $\underline{a}^*$ is in $D[\underline{v}]$ and $\underline{a}$ is in $C[v]$.

Proof: Let $\underline{a}$ be C-state in C[v]. Then there is a partial allowed sequence from v to a such that L[v, a(1), ..., a(k), a] = $\underline{a}$. Then since $\underline{v}$ is in C[u] we also have a partial allowed sequence from u to v such that L[u, v(1), ..., v(t), v] = $\underline{v}$. Thus $\underline{a}^*$ = L[u, v(1), ..., v(t), v, a(1) ..., a(k) a] is a C-state in C[u]. $\underline{a}^*$ is also in D[$\underline{v}$] since $\underline{v} \,\mathfrak{J}\, \underline{a}^*$ and $\underline{a}^* = \underline{v} + \underline{a}$. Hence for every $\underline{a}$ in C[v] there is a corresponding $\underline{a}^*$ in D[$\underline{v}$]. Similarly for every $\underline{a}^*$ in D[$\underline{v}$], since $\underline{v} \,\mathfrak{J}\, \underline{a}^*$, we have a partial allowed sequence from v to a such that L[v, a(1), ..., a(k), a] + $\underline{v}$ = $\underline{a}^*$. Thus there is one-to-one correspondence between the C-states.

We note also that ordering relations in the two lattices C[v] and D[$\underline{v}$] are identical since, by (7:4), the ordering is numerical and numerical ordering is preserved under the transformation $\underline{a}^* = \underline{v} + \underline{a}$ between corresponding elements in C[v] and D[$\underline{v}$]. Hence the lattices are isomorphic.

A corollary to (8:A) is:

(8:2) In a circuit which is sm[u] and sm[u*] if $\underline{v}$ is in C[u] and $\underline{v}^*$ is in C[u*] and t($\underline{v}$) = t($\underline{v}^*$) = v, then D[$\underline{v}$] is isomorphic with D[$\underline{v}^*$] under the transformation $\underline{v}^* + \underline{a} = \underline{v} + \underline{a}^*$, where $\underline{a}$ is in D[$\underline{v}$] and $\underline{a}^*$ is in D[$\underline{v}^*$].

This result follows from (8:A) since D[$\underline{v}$] and D[$\underline{v}^*$] are both isomorphic with C[v]. Theorems (8:A) and (8:2) show that the lattice properties of D[$\underline{v}$] are independent of the initial state u provided, of course, that u $\mathfrak{J}$ v. In other words, the behavior of the circuit after having passed through state v is independent of the initial state u of the circuit and depends only on v. The fact that the numerical components of the vectors in D($\underline{v}$) have their fiducial values altered (by $\underline{v}^* - \underline{v}$) when the initial state is altered, is merely a consequence of the way the C-states are defined and does not reflect a physical property of the circuit. The lattice relations $\mathfrak{J}$, $\cup$, and $\cap$, as well as the $\mathfrak{R}$ relation, are invariant under such translations, as is the circuit behavior which we are seeking to describe with them.

Two properties of recurring states will now be developed.

(8:3) If $\underline{a}$ and $\underline{b}$ are in C[u] and $t(\underline{a}) = t(\underline{b})$, then $t(\underline{a} \cup \underline{b}) = t(\underline{a}) = t(\underline{b})$.

Proof: Let $\underline{c} = \underline{a} \cup \underline{b}$ and let $c = t(\underline{c})$. Then for any component $\underline{c}_i = \max \{ \underline{a}_i, \underline{b}_i \}$. Assume $\underline{a}_i \geq \underline{b}_i$ so $\underline{c}_i = \underline{a}_i$. Then since $\underline{a} \succ \underline{c}$ we may form a partial allowed sequence from $a = t(\underline{a})$ to c, such that $L[a, c(1), \ldots, c(k), c] = \underline{c} - \underline{a}$. Since the i'th component of this vector is zero, the i'th signal has not changed in going from a to c and $a_i = c_i$. Similarly if $\underline{b}_i \geq \underline{a}_i$ we have $b_i = c_i$. But $a_i = b_i = t(\underline{a})_i = t(\underline{b})_i$ so in any case $t(\underline{c})_i = t(\underline{a})_i = t(\underline{b})_i$ for all components and $t(\underline{a} \cup \underline{b}) = t(\underline{a}) = t(\underline{b})$.

(8:4) If $\underline{a}$ and $\underline{b}$ are in C[u] and $a = t(\underline{a})$ and $b = t(\underline{b})$ are in two equivalence sets A and B where $A \overset{\circ}{\succ} B$, then $t(\underline{a} \cup \underline{b})$ is in B.

Proof: By (3:C) $a \overset{\circ}{\succ} b$ so we may form a partial allowed sequence from a to b. Define $\underline{b}^* = \underline{a} + L[a, b(1) \ldots, b(k), b]$, and $t(\underline{b}^*) = b$. Also $\underline{a} \succ \underline{b}^*$. Let $\underline{b}^{**} = \underline{b} \cup \underline{b}^*$. Thus $\underline{a} \succ \underline{b}^{**}$ and $\underline{b} \succ \underline{b}^{**}$ so $\underline{a} \cup \underline{b} \succ \underline{b}^{**}$ and hence $t(\underline{a} \cup \underline{b}) \overset{\circ}{\succ} b$. But since $\underline{b} \succ \underline{a} \cup \underline{b}$, we have $b \overset{\circ}{\succ} t(\underline{a} \cup \underline{b})$ and $t(\underline{a} \cup \underline{b})$ must be in B.

8.2 We now define a set of numerical vectors associated with any C-state which will serve to describe the cycling properties of the circuit.

(8:5a) Given $\underline{v}$ in C[u], we define a set $W[\underline{v}]$ of numerical vectors $w(1), w(2), \ldots, w(k)$, having non-negative integral components by the following rule. $W[\underline{v}]$ contains all non-zero vectors $w(i)$ such that $\underline{v} + w(i)$ is in $E[\underline{v}]$ and if $\underline{a}$ is in $E[\underline{v}]$ with $\underline{v} \succ \underline{a} \succ \underline{v} + w(i)$ then either $\underline{a} = \underline{v}$ or $\underline{a} = \underline{v} + w(i)$.

The statement (8:5a) involves the "covers" concept and, in fact, it may be restated as:

(8:5b) $w(i)$ is in $W[\underline{v}]$ if and only if $\underline{v} + w(i)$ covers $\underline{v}$ in $E[\underline{v}]$.

The set $W[\underline{v}]$ may, of course, be empty, in which case we shall say that $k = 0$. No limit is set on k by the definition but it will appear later that k cannot be greater than n.

Incidentally it may be noted that the components of the vectors w(i) are always even integers since they represent a number of changes in the signals which brings them back to their initial values and the number of negative changes must equal the number of positive changes.

(8:B) If $W[\underline{v}]$ is a set of vectors as defined above,

$$w(i) \vee w(j) = w(i) + w(j) \text{ when } i \neq j.$$

Proof: We must not have $w(i) < w(j)$ for then $\underline{v} < \underline{v} + w(i) < \underline{v} + w(j)$ in violation of (8:5). Hence $w(j) < w(i) \vee w(j)$. By the numerical properties of vectors and using (6:16) $w(i) \vee w(j) \leq w(i) + w(j)$ and hence $\underline{v} + w(j) < \underline{v} + [w(i) \vee w(j)] = [\underline{v} + w(i)] \vee [\underline{v} + w(j)] \leq \underline{v} + w(i) + w(j)$. Let $\underline{v}^* = \underline{v} + w(j)$. We now show that all expressions in this inequality are in $E[\underline{v}^*]$. The expression $[\underline{v} + w(i)] \vee [\underline{v} + w(j)]$ is in $E[\underline{v}]$ by (8:3) but it exceeds $\underline{v}^*$ so it is in $E[\underline{v}^*]$. Also $\underline{v} + w(i) + w(j) = \underline{v}^* + w(i)$ and is in $E[\underline{v}^*]$ by (8:2) with $u = u^*$.

We now write the isomorphic expressions by (8:2) with $u^* = u$. They are $\underline{v} < \underline{v} + [w(i) \vee w(j)] - w(j) \leq \underline{v} + w(i)$ and all expressions are now in $E[\underline{v}]$. Then by (8:5b) we obtain $[w(i) \vee w(j)] - w(j) = w(i)$.

In order for the relation $w(i) \vee w(j) = w(i) + w(j)$ to hold for vectors having non-negative components the non-zero components of w(i) and w(j) must have distinct component indices. Since this is true for all pairs of vectors in $W[\underline{v}]$ we have:

(8:6) The vectors w(1), w(2), ..., w(k) of $W[\underline{v}]$ all have distinct indices for their non-zero components.

In other words, if $w_m(i) > 0$, then $w_m(j) = 0$ for all $j \neq i$. This also means that the vectors of $W[\underline{v}]$ are orthogonal in the vector sense, i.e., the inner product of w(i) and w(j) is zero if and only if $i \neq j$.

A consequence of (8:6) is the restriction $k \leq n$ which was mentioned earlier. In case $k = n$ each w(i) has just one non-zero component and one w(i) would correspond to each component index.

We shall describe the component indices of the non-zero components of w(i) as the set of component indices spanned by w(i). Furthermore, we shall designate the set of component indices spanned by any of the k vectors of $W[\underline{v}]$ as the set of component indices spanned by $W[\underline{v}]$.

(8:C) The set $E[\underline{v}]$ is precisely the set of vectors $\underline{x}$ which may be expressed in the form:

(8:7) $\underline{x} = \underline{v} + \sum_{i=1}^{k} a_i\, w(i)$ where the coefficients a_i are allowed to run over the non-negative integers.

Proof: If $\underline{x} = \underline{v} + \sum_{i=1}^{k} a_i\, w(i)$ then we show that $\underline{x}$ is in $E[\underline{v}]$ by induction. Certainly $\underline{x} = \underline{v}$ is in $E[\underline{v}]$, which is the case in which the coefficients a_i are all zero. Assume next that $\underline{x} = \underline{v} + \sum_{i=1}^{k} a_i\, w(i)$ is in E[v] for a given set of coefficients a_i. Since $t(\underline{v}) = t(\underline{x})$ then by (8:2) with u = u* we have $\underline{x} + w(j)$ is in $E[\underline{x}]$ since $\underline{v} + w(j)$ is in $E[\underline{v}]$. Hence $\underline{x} + w(j)$ is in $E[\underline{v}]$ and we see that any coefficient a_j may be increased by 1 (and hence by any integer) to yield a new $\underline{x}$ in $E[\underline{v}]$.

Next assume that $\underline{x}$ is in $E[\underline{v}]$. Induction is used to show that $\underline{x}$ may be expressed in form (8:7). Form a covering sequence of C-states in $E[\underline{v}]$ from $\underline{v}$ to $\underline{x}$. (This is shown to be possible in Ref. 3 page 6.) Let us assume that some member $\underline{y}$ of this sequence may be expressed in form (8:7). We note that $\underline{v}$ is such a member. Let $\underline{z}$ be the next member of the sequence after $\underline{y}$ so that $\underline{z}$ covers $\underline{y}$ in E[v]. Then by (8:2) $\underline{v} + (\underline{z} - \underline{y})$ covers $\underline{v}$ and hence by (8:5b) we see that $(\underline{z} - \underline{y})$ is one of the vectors w(i) in $W[\underline{v}]$. Since $\underline{z} = \underline{y} + w(i)$ we see that $\underline{z}$ is also expressible in form (8:7) and by induction so is $\underline{x}$.

Cycling with respect to the set $E[\underline{v}]$ is completely described by (8:C) since we see that v has periodicity of multiplicity k.

8.3 We now turn to the investigation of the dependence of $W[\underline{v}]$ on $\underline{v}$.

(8:8) If $\underline{v}$ is in C[u] and $\underline{v}$* is in C[u*] and v = $t(\underline{v}) = t(\underline{v}^*)$, then $W[\underline{v}] = W[\underline{v}^*]$.

Proof: By (8:2) $D[\underline{v}]$ is isomorphic with $D[\underline{v}^*]$ under the transformation $\underline{v}^* + \underline{a} = \underline{v} + \underline{a}^*$. We see that since the $w(i)$ in $W[\underline{v}]$ are differences between members of $D[\underline{v}]$ they are invariant under the transformation.

We shall therefore be able to write $W[v]$ to represent $W[\underline{v}]$ for all $\underline{v}$ such that $t(\underline{v}) = v$.

(8:D) In an sm[u] circuit if $u \mathfrak{F} a \mathfrak{F} b$, then any member of $W[a]$ is a sum of one or more members of $W[b]$.

Proof: Since $u \mathfrak{F} a \mathfrak{F} b$ we may construct partial allowed sequences from u to a to b and thereby define some C-states $\underline{a}$ and $\underline{b}$ as $\underline{a} = L[u, a(1), \ldots, a(p), a]$ and $\underline{b} = \underline{a} + L[a, b(1), \ldots, b(q), b]$. We have defined $\underline{a}$ and $\underline{b}$ so that $a = t(\underline{a})$ and $b = t(\underline{b})$ and $\underline{a} \mathfrak{F} \underline{b}$. Thus $\underline{b}$ is in $D[\underline{a}]$. By (8:2) if $w(j, a)$ is in $W[\underline{a}]$ then $D[\underline{a}]$ is isomorphic with $D[\underline{a} + w(j, a)]$ and thus we have a correspondence between $\underline{b}$ and $\underline{b} + w(j, a)$. Hence $\underline{b} + w(j, a)$ is in $E[\underline{b}]$ and must be expressible in form (8:7), so that $w(j, a)$ may be written in the form $w(j, a) = \sum_{i=1}^{k} c_i\, w(i, b)$ where the c_i's are non-negative integers, not all zero, and the vectors $w(i, b)$ are the members of $W[\underline{b}]$. Now since $W[a] = W[\underline{a}]$ and $W[b] = W[\underline{b}]$ we have proved (8:D).

A corollary to (8:D) is the result that the number k of vectors can never decrease while passing through an allowed sequence. Thus, k has in common with entropy the property of never decreasing with time. It is also apparent that indices once spanned by a vector $w(i)$ will remain spanned throughout the remainder of an allowed sequence.

Our picture of the behavior of a semi-modular circuit as it passes through an allowed sequence now involves an increasing number of vectors $w(i)$ being introduced and increasingly more indices being spanned. Also, we may imagine old vectors $w(i)$ breaking up into several vectors, each one spanning fewer nodes than the old $w(i)$.

(8:E) In an sm[u] circuit if $u \mathfrak{F} a$ and a and b are in the same equivalence set A, then $W[a] = W[b]$.

Proof: Since $a \mathfrak{J} b$ if $w(i, a)$ is in $W[a]$, then by (8:D), $w(i, a)$ is a sum of one or more members of $W[b]$, so if $w(j, b)$ is in this sum, we have $w(i, a) \geq w(j, b)$, since the vectors have non-negative components. Similarly, since $b \mathfrak{J} a$ there is a $w(h, a)$ in $W[a]$ such that $w(j, b) \geq w(h, a)$. But by (8:6), if $w(i, a) \geq w(h, a)$, we must have $h = i$ and $w(i, a) = w(h, a)$, and hence $w(i, a) = w(j, b)$. Hence, for every $w(i, a)$ in $W[a]$ there is an equal $w(j, b)$ in $W[b]$, and similarly for every $w(j, b)$ in $W[b]$ there is an equal $w(i, a)$ in $W[a]$. Thus the two sets contain exactly the same vectors and $W[a] = W[b]$.

This means we may write $W[A]$ to represent the set of vectors corresponding to the equivalence set A. The set of vectors $w(i)$ now appears as a function of equivalence sets where originally it was defined as a function of C-states. We shall also use the notation $\underline{a}$ contained in $\underline{A}$ to denote that $t(\underline{a})$ is an element of the equivalence set A. Finally we shall say that a component i is unspanned by $W[A]$ if and only if the i'th component of a C-state in $\underline{A}$ is unspanned by any of the vectors $w(j)$ of $W[A]$.

(8:F) $\underline{a}$ and $\underline{b}$ both lie in $\underline{A}$ if and only if those components of $\underline{a}$ and $\underline{b}$ unspanned by $W[A]$ are identical.

Proof: Assume a and b are in the same equivalence set A. Form $\underline{c} = \underline{a} \cup \underline{b}$. By (8:4) we have $c = t(\underline{c})$ also in A. Hence $c \mathfrak{J} a$, and we may construct a partial allowed sequence from c to a and define $\underline{a}^* = \underline{c} + L[c, a(1), \ldots, a(r), a]$. Since $\underline{a} \mathfrak{J} \underline{c} \mathfrak{J} \underline{a}^*$ we have $\underline{a}_j \leq \underline{c}_j \leq \underline{a}_j^*$ for each component index j. Now $\underline{a}^* = \underline{a} + \sum_{i=1}^{k} q_i\, w(i)$ by (8:C), so for those components $\underline{a}_j$ not spanned by the $w(i)$'s we have $\underline{a}_j = \underline{a}_j^*$, and hence $\underline{a}_j = \underline{c}_j$ for unspanned components. Similarly $\underline{b}_j = \underline{c}_j$ for unspanned components, giving $\underline{a}_j = \underline{b}_j$.

Assume now that $\underline{a}$ and $\underline{b}$ have identical unspanned components. Let $\underline{b}_{i\ max}$ be the largest spanned component of $\underline{b}$. If no components are spanned let $b_{i\ max} = 0$. Then form $\underline{a}^* = \underline{a} + \underline{b}_{i\ max} \sum_{i=1}^{k} w(i)$ where the $w(i)$ are taken from $W[\underline{a}]$. Then

$\underline{b} \mathcal{J} \underline{a}^*$, so $b \mathcal{J} a$ by (8:C). Similarly we have $a \mathcal{J} b$.

(8:G) If $\underline{a}$ and $\underline{b}$ lie in $\underline{A}$ and index i is unspanned by W[A], then

$\underline{a}_i' = \underline{b}_i'$.

Proof: We begin by proving that $a_i' = b_i'$. Construct a partial allowed sequence a, a(1), a(2), ..., a(p), a, which contains all states in A by the method given in the proof of (5:C). We notice that a', a'(1), a'(2), ..., a'(p), a' is an $\mathcal{R}$-sequence, because by (5:3) $a(j) \mathcal{R} a(j+1)$ implies $a(j+1) \mathcal{R} a'(j)$ and hence $a'(j) \mathcal{R} a'(j+1)$ for each i = 1, 2, ..., p - 1 and similarly $a' \mathcal{R} a'(1)$ and $a'(p) \mathcal{R} a'$. (It may not be a partial allowed sequence since some consecutive pairs may be equal.) By our hypothesis index i is unspanned by W[A] so that $a_i = a_i(1) = a_i(2) = \dots = a_i(p)$. Assume that $a_i < a_i'$. Then $a_i = a_i(1) < a_i' \leq a_i'(1)$ and in general $a_i(j+1) < a_i'(j) \leq a_i'(j+1)$. Thus we have $a_i' \leq a_i'(1) \leq a_i'(2) \leq \dots \; a_i'(p) \leq a_i'$, so that $a_i' = a_i'(j)$ for all j = 1, 2, ..., p. Similarly $a_i' = a_i'(j)$ for all j = 1, 2, ..., p if we assume $a_i > a_i'$.

In the remaining case $a_i = a_i'$, if j exists such that $a_i(j) \neq a_i'(j)$ then by the previous argument we have $a_i' = a_i'(j)$, giving the contradiction $a_i' = a_i' = a_i'(j) \neq a_i(j) = a_i$. Therefore, in this case, too, we have $a_i' = a_i'(j)$ for all j = 1, 2, ..., p. But since all states of A are included in the sequence a, a(1), a(2), ..., a(p), a we see that $a_i' = b_i'$ for any pair of states in A.

Now let $\underline{a}$ and $\underline{b}$ be any two C-states in $\underline{A}$. Then $\underline{a}' = \underline{a} + L[a, a']$ and $\underline{b}' = \underline{b} + L[b, b']$. But $\underline{a}_i = \underline{b}_i$ by (8:F) and $|a_i' - a_i| = |b_i' - b_i|$ so $\underline{a}_i' = \underline{b}_i'$.

Two corrolaries are immediate; they are

(8:9) For any $\underline{a}$ in $\underline{A}$ there exists a unique $\underline{A}'$ for which $\underline{a}'$ is in $\underline{A}'$ and $A \mathcal{J} A'$.

(8:10) If A is final and i is unspanned by W[A] then $\underline{a}_i = \underline{a}_i'$ for any $\underline{a}$ in A.

Thus we see that the unspanned components of the C-states and, hence, the unspanned signals of the states, characterize the equivalence sets. Within equivalence sets only spanned components and signals change, while in going from one equivalence set to another the unspanned components and signals must change. In such a transition the number of unspanned components may decrease, and if it does the number k of vectors must increase. It is possible as we shall see later, for the number k of vectors to increase, without having a decrease in the number of unspanned components.

It also should be observed that the unspanned signals of the states uniquely determine the unspanned components of the C-states, since these are fixed by the equivalence set.

8.4 As an example consider the circuit defined by the equations

(8:11)
$$\begin{aligned} z_1' &= 1 \\ \bar{z}_2' &= \bar{z}_1\bar{z}_3 \vee z_1\bar{z}_2 \\ z_3' &= \bar{z}_1 z_2 \vee z_1\bar{z}_3 \end{aligned}$$

If the circuit is started in the initial state u = (0, 0, 0) it may be shown to be semi-modular. Two equivalence sets occur. They may be designated A and B as follows: A contains (0, 0, 0), (0, 1, 0), 0, 1, 1), (0, 0, 1); B contains (1, 0, 0), (1, 1, 0), (1, 1, 1), (1, 0, 1). In the circuit $A \mathfrak{F} B$, so B is a final set. The first signal is the only one unspanned by vectors w(i) in either set. W[A] contains just one vector (0, 2, 2). W[B] contains [0, 2, 0] and [0, 0, 2]. Here we have an example of a single vector from W[A] splitting into two in W[B]. In this case the same number of unspanned signals occurs in both A and B but this will not be the case in general.

9. Ideals of C[u]

9.1 While investigating the behavior of asynchronous circuits one is often

concerned with what happens if a signal fails to change if it is supposed to do so. Malfunctions of this type never lead to C-states which are not in C[u], since no assumptions have been made about the relative speeds of the elements.

Another problem, which is of interest to the circuit designer, is to find a way of describing the apparent behavior of a circuit to an observer who is not aware of all the signals which are present, but "sees" only certain signals from among the entire set. This problem and the preceding one will be treated by investigating the ideals of C[u].

9.2 In order to represent the ideals of C[u], we introduce the notion of a C-signal. This concept will also be useful in the theory of distributive circuits, which are treated in section 10.

(9:1) For each pair of integers α and i, such that there exists at least one C-state $\underline{a}$ in C[u] for which $\underline{a}_i = \alpha$, we define the C-signal (α, i) as the set of all C-states $\underline{b}$ in C[u] having $\underline{b}_i \leq \alpha$. The C-state $\underline{a}$ is then said to induce the C-signal (α, i).

The C-signal (α, i) thus refers to the αth change which has occurred at point i in the circuit and, more specifically, contains all C-states in C[u] for which no more than α signal changes have occurred at point i. It therefore describes the possible C-states which may occur if point i is prevented from changing more than α times. To describe what may happen if several signals fail to change we introduce the notion of a break set.

(9:2) If a C-state $\underline{a}$ in C[u] induces all the distinct C-signals $(\alpha_1, i_1), (\alpha_2, i_2), \ldots, (\alpha_m, i_m)$, we define the break set $\underline{\alpha} = [(\alpha_1, i_1), (\alpha_2, i_2), \ldots, (\alpha_m, i_m)]$ as the set of all C-states $\underline{b}$ having $\underline{b}_{i_j} \leq \alpha_j$ for j = 1, 2, ..., m. The C-state $\underline{a}$ is then said to induce the break set $\underline{\alpha}$.

It will appear later that m cannot be greater than n, since in (9:4) it is shown that the indices i_j are distinct. We shall, however, admit the possibility

that m = 0 as a special case. This break set $\underline{\theta}$ = [ ] will be taken equal to C[u] and all C-states in C[u] will be said to induce it.

We note that the C-signals are, themselves, break sets referring to single C-signals. In other words, $[(\alpha, i)] = (\alpha, i)$.

(9:3) If for each of the m C-signals (α_j, i_j), where $j = 1, 2, \ldots, m$, there is a C-state $\underline{a}(j)$ inducing (α_j, i_j) and contained in the other C-signals, then $\underline{\alpha} = [(\alpha_1, i_1), (\alpha_2, i_2), \ldots, (\alpha_m, i_m)]$ is a break set.

This follows from (9:2) if we let $\underline{a} = \underline{a}(1) \cup \underline{a}(2) \cup \ldots \cup \underline{a}(m)$.

(9:4) If $\underline{\alpha} = [(\alpha_1, i_1), (\alpha_2, i_2), \ldots (\alpha_m, i_m)]$ is any break set, the signal indices $i_1, i_2, \ldots, i_m$ are distinct.

<u>Proof</u>: Let $\underline{a}$ induce $\underline{\alpha}$. If $i_p = i_q$, then by (9:2) $\alpha_p = \underline{a}_{i_p} = \underline{a}_{i_q} = \alpha_q$, which conflicts with the assumption that the C signals are distinct.

(9:A) Any break set is an ideal of C[u].

<u>Proof</u>: Ideals of C[u] are defined as non-empty subsets of C[u] having the following two properties.

(9:5a) An ideal J contains $\underline{x} \cup \underline{y}$ if it contains $\underline{x}$ and $\underline{y}$.

(9:5b) If $\underline{x}$ and $\underline{y}$ are C-states in C[u], and if $\underline{x}$ is in an ideal J, then $\underline{x} \cap \underline{y}$ is also in J.

Property (9:5a) also applies to break sets by (7:5). We may infer (9:5b) from (7:4) and the fact that $\underline{x} \cap \underline{y} \Im \underline{x}$.

(9:B) Any ideal of C[u] can be represented as a break set in at least one way.

<u>Proof</u>: Let J be an ideal of C[u]. It should be noted that since J is non-empty it must contain at least the C-state $\underline{0}$, whose components are all zero. List all C-signals $(\alpha_1, i_1), (\alpha_2, i_2), \ldots, (\alpha_m, i_m)$ such that (α_j, i_j) is induced by some C-state $\underline{a}(j)$ in J, where there is no C-signal (β_j, i_j) with $\beta_j > \alpha_j$ which is

induced by a C-state in J (i.e. α_j is maximal). Our list may contain no more than n C-signals by virtue of its definition, and if some index i_{m+1} is not represented in the list then every C-signal (α_{m+1}, i_{m+1}) is induced by a C-state in J since $(0, i_{m+1})$ is induced by $\underline{0}$ in J. Let the C-states in J inducing these C-signals be denoted by $\underline{a}(1)$, $\underline{a}(2)$, ..., $\underline{a}(m)$. If $m > 0$ we have $\underline{a} = \underline{a}(1) \cup \underline{a}(2) \cup \ldots \cup \underline{a}(m)$ in J by (9:5a), and from the construction of each $\underline{a}(j)$ we see that $\underline{a}$ induces a break set $\underline{\alpha} = [(\alpha_1, i_1), (\alpha_2, i_2), \ldots, (\alpha_m, i_m)]$. By (9:2) $\underline{\alpha}$ contains J. If $m = 0$ we let $\underline{\alpha} = \Theta = C[u]$, which must contain J.

To show that J contains $\underline{\alpha}$, let $\underline{x}$ be a C-state in $\underline{\alpha}$. Now for each component $\underline{x}_p$ of $\underline{x}$ we can find a C-state $\underline{b}(p)$ in J such that $\underline{b}_p(p) \geq \underline{x}_p$. Let $\underline{b} = \underline{b}(1) \cup \underline{b}(2) \cup \ldots \cup \underline{b}(n)$. Then $\underline{b}$ is in J by (9:5a). But $\underline{x} \mathcal{F} \underline{b}$ so $\underline{x} = \underline{x} \cap \underline{b}$ is in J by (9:5b). Hence J contains $\underline{\alpha}$ so $J = \underline{\alpha}$.

9.3 We see from (9:A) and (9:B) that the break set notation is simply a way of specifying ideals. It is well known that the ideals of C[u] form a lattice. The relationship of this lattice to C[u] is expressed in (9:6).

(9:6) The ideals of C[u] form a lattice under set inclusion. In this lattice $\underline{\alpha} \cup \underline{\beta}$ is the set of all elements of the form $(\underline{a} \cup \underline{b}) \cap \underline{c}$, where $\underline{a}$ and $\underline{b}$ are in $\underline{\alpha}$ and $\underline{\beta}$ respectively, and $\underline{c}$ is any C-state. The ideal $\underline{\alpha} \cap \underline{\beta}$, on the other hand, is merely the set theoretical meet, containing all elements in both $\underline{\alpha}$ and $\underline{\beta}$.

9.4 Various subsets of the lattice of ideals are important from the point of view of circuit behavior. One such subset is defined by (9:7).

(9:7) $H[u; i_1, i_2, \ldots, i_m]$ is the set of ideals of C[u] which may be represented in the form $\underline{\alpha} = [(\alpha_1, i_1), (\alpha_2, i_2), \ldots, (\alpha_m, i_m)]$ where the quantities α_j may range over all values permitted by (9:2).

This set may be regarded as describing the behavior of the circuit to an observer who merely detected the signals at point $i_1, i_2, \ldots, i_m$. To such an

observer the ideals of $H[u; i_1, i_2, \ldots, i_m]$ would correspond to the C-states of an ordinary observer. Such sets also provide the basis for a theory of equivalent circuits. Two circuits could be called equivalent if $H[u; i_1, i_2, \ldots, i_m]$ in the first circuit is the same as $H[v; j_1, j_2, \ldots, j_m]$ in the second circuit. This type of equivalence is defined with respect to initial states u and v and selected signal indices in the two circuits.

The set $H[u; 1, 2, \ldots, n]$ is isomorphic with the lattice $C[u]$, where set inclusion replaces the $\mathfrak{J}$ relationship. Also $H[u, i]$ is merely a chain. Our suspicion that $H[u; i_1, i_2, \ldots, i_m]$ is a lattice under set inclusion will be shown to be justified, but it is not necessarily a sub-lattice of the lattice of ideals. We begin with lemma (9:8) which is analogous to (7:4).

(9:8) If $\underline{\alpha}$ and $\underline{\beta}$ are in $H[u; i_1, i_2, \ldots, i_m]$ then $\underline{\alpha} \subseteq \underline{\beta}$ if and only if $\alpha_j \leq \beta_j$ for $j = 1, 2, \ldots, m$.

<u>Proof</u>: If $\alpha_j \leq \beta_j$ for $j = 1, 2, \ldots, m$ we see by (9:2) that $\underline{\alpha} \subseteq \underline{\beta}$. If $\underline{a}$ induces $\underline{\alpha}$, we have $\underline{a}_{i_j} = \alpha_j$. If, now, $\underline{\alpha} \subseteq \underline{\beta}$ we also have $\underline{a}$ in $\underline{\beta}$; hence $\underline{a}_{i_j} \leq \beta_j$ for $j = 1, 2, \ldots, m$, and therefore $\alpha_j \leq \beta_j$ for $j = 1, 2, \ldots, m$.

(9:C) $H[u; i_1, i_2, \ldots, i_m]$ is a lattice under set inclusion.

<u>Proof</u>: Let $\underline{\alpha}$ and $\underline{\beta}$ be two ideals in $H[u; i_1, i_2, \ldots, i_m]$. Define $\underline{\gamma}$ by the relationship $\gamma_j = \max[\alpha_j, \beta_j]$ for $j = 1, 2, \ldots, m$. We see that $\underline{\gamma}$ is an ideal in $H[a; i_1, i_2, \ldots, i_m]$, since if $\underline{a}$ and $\underline{b}$ induce $\underline{\alpha}$ and $\underline{\beta}$ respectively $\underline{a} \cup \underline{b}$ must induce $\underline{\gamma}$ by (7:5). By (9:8) $\underline{\gamma}$ contains $\underline{\alpha}$ and $\underline{\beta}$. It is also a least upper bound in $H[u; i_1, i_2, \ldots, i_m]$ since any other upper bound must contain $\underline{\gamma}$ by (9:8).

To show that $\underline{\alpha}$ and $\underline{\beta}$ have a greatest lower bound in $H[u; i_1, i_2, \ldots, i_m]$ we follow an argument similar to that of (7:6). Let $\underline{\omega} = [(0, i_1), (0, i_2), \ldots, (0, i_m)]$ be the ideal in $H[u; i_1, i_2, \ldots, i_m]$ induced by the C-state $\underline{0}$. By (9:8) we see that $\underline{\omega}$ is a lower bound to $\underline{\alpha}$ and $\underline{\beta}$ and thus there is at least one lower bound. Now if we form the least upper bound of all lower bounds to $\underline{\alpha}$ and $\underline{\beta}$ we see that the result must be the greatest lower bound by the construction of the previous paragraph and (9:8).

A result analogous to (7:C) may also be obtained for the set $H[u ; i_1, i_2, \ldots, i_m]$.

(9:D) $\underline{\alpha}$ covers $\underline{\beta}$ in $H[u; i_1, i_2, \ldots, i_m]$ if and only if there is one index i_j such that $\alpha_j = \beta_j + 1$ and $\alpha_p = \beta_p$ whenever $i_p \neq i_j$.

<u>Proof</u>: If $\alpha_j = \beta_j + 1$ and $\alpha_p = \beta_p$ whenever $i_p \neq i_j$ then $\underline{\alpha}$ must cover $\underline{\beta}$ in $H[u; i_1, i_2, \ldots, i_m]$ by (9:8), since all the quantities involved are integers.

Next assume that $\underline{\alpha}$ covers $\underline{\beta}$. To complete the proof we require the lemma (9:9) which is valid for any ideal $\underline{\alpha}$.

(9:9) If $\underline{b}$ is in $\underline{\alpha}$ and $\underline{a}$ induces $\underline{\alpha}$ then $\underline{a} \cup \underline{b}$ induces $\underline{\alpha}$.

Since $\alpha_j = \underline{a}_{i_j}$ and $\alpha_j \geq \underline{b}_{i_j}$ by (9:2) we have $\underline{b}_{i_j} \leq \underline{a}_{i}$ and $\underline{a}_{i_j} \vee \underline{b}_{i_j} = \alpha_j$ so $\underline{a} \cup \underline{b}$ induces $\underline{\alpha}$.

Returning to the original proof we let $\underline{a}$ and $\underline{b}$ be two C-states inducing $\underline{\alpha}$ and $\underline{\beta}$ respectively, and by (9:9), $\underline{a} \cup \underline{b}$ induces $\underline{\alpha}$. Since $\underline{b} \neq \underline{a} \cup \underline{b}$, we may form a covering sequence $\underline{b}$, $\underline{c}(1)$, ..., $\underline{c}(p)$, $\underline{a} \cup \underline{b}$. Let $\underline{c}(i)$ be the last C-state in the sequence which induces $\underline{\beta}$. By (9:8) all previous C-states in the sequence induce $\underline{\beta}$ and all later C-states induce $\underline{\alpha}$ and no other ideals in $H[u; i_1, i_2, \ldots, i_m]$ may be induced by members of the sequence. Since $\underline{c}(i)$ and $\underline{c}(i + 1)$ differ by one in just one component, by (7:C), we see that $\underline{\beta}$ and $\underline{\alpha}$ may differ in no more than one C-signal, and in that, by at most one. But since $\underline{\beta}$ and $\underline{\alpha}$ are different ideals we obtain (9:D).

9.5 A correspondence between equivalence sets and certain ideals will now be developed which permits us to predict the behavior of a circuit in which certain signal changes are arrested. In particular, we shall be interested in determining whether or not the circuit will stop if certain signal changes fail to occur when they are expected to do so.

These questions are treated by considering the subset of the ideals defined in (9:10).

(9:10) K[u] is the set of all ideals $\underline{\alpha} = [(\alpha_1, i_1), (\alpha_2, i_2), \ldots, (\alpha_m, i_m)]$ such that there exists a C-state $\underline{a}$ inducing $\underline{\alpha}$ whose unspanned component indices are just $i_1, i_2, \ldots, i_m$.

Again if there is a C-state $\underline{a}$, having no unspanned component indices, we shall assume the convention that $\theta = [\ ]$ is a member of K[u].

(9:E) The partially ordered set of equivalence sets A, B, ... which follow U (the equivalence set of u) is isomorphic with K[u], where the $\mathfrak{F}$ relationship corresponds to set inclusion.

Proof: Let $\underline{a}$ be in $\underline{A}$ and let $\underline{a}$ induce $\underline{\alpha}$ in K[u]. By (8:F) we see that every other C-state in $\underline{A}$ also induces $\underline{\alpha}$. Thus for every equivalence set A, B, ... there is a corresponding ideal in K[u], and by definition (9:10) there is an equivalence set for every ideal in K[u].

We now show the correspondence between the $\mathfrak{F}$ relationship over sets A, B, ... and set inclusion over K[u]. Given $\underline{\beta} \subseteq \underline{\alpha}$ with $\underline{\alpha}$ and $\underline{\beta}$ in K[u], then if $\underline{a}$ induces $\underline{\alpha}$ and $\underline{b}$ induces $\underline{\beta}$, we have $\underline{a} \cup \underline{b}$ induces $\underline{\alpha}$, by (9:9). Since $\underline{b}\ \mathfrak{F}\ \underline{a} \cup \underline{b}$, we have $B\ \mathfrak{F}\ A$.

Assume next that $B\ \mathfrak{F}\ A$, where $U\ \mathfrak{F}\ B$. Let a be a state in A and b a state in B. Form C-states $\underline{b} = L[u, \ldots, b]$ and $\underline{a} = \underline{b} + L[b, \ldots, a]$. We thus have $\underline{a}$ in $\underline{A}$ and $\underline{b}$ in $\underline{B}$, with $\underline{b}\ \mathfrak{F}\ \underline{a}$. Now by (8:D), the unspanned indices of A are also unspanned in B, so each index i_j of $\underline{\alpha}$ is also present in $\underline{\beta}$. Since $\underline{b}\ \mathfrak{F}\ \underline{a}$ with $\underline{b}$ inducing $\underline{\beta}$ and $\underline{a}$ inducing $\underline{\alpha}$ we have $\beta_j \leq \alpha_j$ for each α_j of $\underline{\alpha}$. Thus $\underline{\beta} \subseteq \underline{\alpha}$ by (9:2).

This latter argument may also be used in proving (9:11).

(9:11) If $\underline{b}$ is in $\underline{\alpha}$ and induces $\underline{\beta}$, where $\underline{\alpha}$ and $\underline{\beta}$ are both in K[u], then $\underline{\beta} \subseteq \underline{\alpha}$.

Proof: If $\underline{a}$ induces $\underline{\alpha}$, then $\underline{a} \cup \underline{b}$ induces $\underline{\beta}$ by (9:9) and since $\underline{b}\ \mathfrak{F}\ \underline{a} \cup \underline{b}$ we see that $\underline{\alpha}$ and $\underline{\beta}$ are related as in the previous argument with $\underline{a} \cup \underline{b}$ replacing $\underline{a}$.

(9:F) K[u] is a lattice under set inclusion.

Proof: Let $\underline{\alpha}$ and $\underline{\beta}$ be two ideals in K[u], and let $\underline{\gamma}$ be the ideal in K[u] induced by $\underline{a} \cup \underline{b}$, where $\underline{a}$ and $\underline{b}$ induce $\underline{\alpha}$ and $\underline{\beta}$ respectively. By (8:D) the unspanned indices of $\underline{a} \cup \underline{b}$ are also unspanned in $\underline{a}$ and $\underline{b}$, so $\underline{\gamma}$ is independent of which $\underline{a}$ and $\underline{b}$ are chosen. Also, since $\underline{a}$ and $\underline{b}$ are in $\underline{\gamma}$, we have $\underline{\alpha} \subseteq \underline{\gamma}$ and $\underline{\beta} \subseteq \underline{\gamma}$, by (9:11). Let $\underline{\delta}$ be any other ideal in K[u] satisfying $\underline{\alpha} \subseteq \underline{\delta}$ and $\underline{\beta} \subseteq \underline{\delta}$. Then $\underline{\delta}$ must contain $\underline{a} \cup \underline{b}$ by (9:5a), and hence $\underline{\gamma} \subseteq \underline{\delta}$ by (9:11). Thus $\underline{\gamma}$ is the least upper bound of $\underline{\alpha}$ and $\underline{\beta}$ in K[u].

Let $\underline{\mu}$ be the ideal of K[u] corresponding to U (the set of u). Thus $\underline{\mu} \subseteq \underline{\alpha}$ and $\underline{\mu} \subseteq \underline{\beta}$ by (9:E), and $\underline{\mu}$ is a lower bound to $\underline{\alpha}$ and $\underline{\beta}$. The least upper bound of all lower bounds to $\underline{\alpha}$ and $\underline{\beta}$ is their greatest lower bound by (9:11).

From the preceding discussion we see that the sets K[u] and H[u; i_1, i_2, ..., i_m] are similar in many of their characteristics. The lemmas (9:8) and (9:11) may be regarded as analogous and the proofs of (9:C) and (9:F) show that the rules for forming least upper bounds are the same. Nothing corresponding to (9:D) can be obtained for K[u], however.

Let us now take an arbitrary ideal $\underline{\gamma} = [(\gamma_1, i_1), (\gamma_2, i_2) \ldots, (\gamma_m, i_m)]$ of C[u]. We may regard $\underline{\gamma}$ as representing those C-states which may occur if the signals at points i_1, i_2, ..., i_m in the circuit are prevented from undergoing more than γ_1, γ_2, ..., γ_m changes. If $\underline{\gamma}$ is a principal ideal, and hence has a maximum C-state, the circuit will stop when this C-state is reached. We now wish to see what conditions must be placed on $\underline{\gamma}$ to require that it be a principal ideal.

(9:12) K[u; $\underline{\gamma}$] is the set of all ideals $\underline{\alpha}$ in K[u] such that there is a C-state $\underline{a}$ in $\underline{\gamma}$ which induces $\underline{\alpha}$.

This means that K[u; $\underline{\gamma}$] corresponds to the set of equivalence sets which have representative C-states in $\underline{\gamma}$.

(9:13) If $\underline{\alpha}$ and $\underline{\beta}$ are both in K[u; $\underline{\gamma}$], then their least upper bound in K[u] is also in K[u; $\underline{\gamma}$].

Proof: Let $\underline{a}$ and $\underline{b}$ both lie in $\underline{\gamma}$, where $\underline{a}$ induces $\underline{\alpha}$ and $\underline{b}$ induces $\underline{\beta}$. Then $\underline{a} \cup \underline{b}$ is also in $\underline{\gamma}$, but $\underline{a} \cup \underline{b}$ induces the least upper bound of $\underline{\alpha}$ and $\underline{\beta}$, by the proof of (9:F), so it is also in K[u; $\underline{\gamma}$].

Since the number of equivalence sets is finite, we see that K[u; $\underline{\gamma}$] contains a finite number of ideals. This implies (9:14).

(9:14) There is a maximum ideal $\underline{\phi}$ in K[u; $\underline{\gamma}$].

Corresponding to this maximum ideal $\underline{\phi}$ there is an equivalence set F which must follow all other equivalence sets represented in $\underline{\gamma}$. Thus we see that if the circuit is constrained to remain in $\underline{\gamma}$, it will eventually reach F. Whether the circuit will stop or not when it reaches F will depend on whether or not cycling can occur in F.

(9:G) $\underline{\gamma}$ is a principal ideal if and only if each w(j) in W[F] has at least one component index of a non-zero component which is represented in $\underline{\gamma}$.

Proof: Assume $\underline{\gamma}$ is a principal ideal. Then its maximum element $\underline{f}$ is in $\underline{F}$. If w(j) has no non-zero component index represented in $\underline{\gamma}$, then $\underline{f}$ + w(j) is also in $\underline{\gamma}$, contradicting the assumption that $\underline{f}$ is maximal.

Assume next that each w(j) has at least one non-zero component index i_j represented in $\underline{\gamma}$. Let (γ_j, i_j) be the corresponding C-signal. Then if $\underline{f}$ is any C-state in $\underline{F}$ we see that no C-state in $\underline{F}$ and $\underline{\gamma}$ can exceed $\underline{f} + \sum_{j=1}^{k} \gamma_j \, w(j)$ without violating (9:2). Thus a maximal C-state in $\underline{\gamma}$ exists and since $\underline{\gamma}$ is an ideal it is unique.

This result allows us to predict whether or not cycling may occur within $\underline{\gamma}$ provided we know the unspanned indices and C-signal corresponding to each equivalence set and the vectors w(j).

9.6 The following example of a binary, semi-modular circuit shows that equivalence sets are not necessarily lattices of C-states and that K[u] need not be a sublattice of the lattice of ideals.

This circuit is represented by the Boolean equations:

$$\dot{z}'_1 = \bar{z}_3 \vee \bar{z}_1 \tag{9:15}$$

$$\dot{z}'_2 = \bar{z}_3 \vee \bar{z}_2$$

$$\dot{z}'_3 = z_1 \vee z_2 \vee z_3$$

Let the initial state u be (0, 0, 0). A partial lattice diagram of C-states may be drawn as follows:

$$\begin{tikzcd}
 & & & (0,0,0) \arrow[dl] \arrow[dr] & & & \\
 & & (1,0,0) \arrow[dl] \arrow[dr] & & (0,1,0) \arrow[dl] \arrow[dr] & & \\
 & (1,0,1) \arrow[d] \arrow[drr] & & (1,1,0) \arrow[d] & & (0,1,1) \arrow[d] \arrow[dll] & \\
 & (2,0,1) \arrow[dl] \arrow[dr] & & (1,1,1) \arrow[dl] \arrow[dr] & & (0,2,1) \arrow[dl] \arrow[dr] & \\
(3,0,1) & & (2,1,1) & & (1,2,1) & & (0,3,1)
\end{tikzcd}$$

Figure 3

The diagram should be continued downward in an infinite, two dimensional array of C-states. Five equivalence sets are present corresponding to the four individual states (0, 0, 0), (1, 0, 0), (0, 1, 0), (1, 1, 0) and the set of states (1, 0, 1), (0, 1, 1), (0, 0, 1), (1, 1, 1). The latter set has two minimal C-states inducing its ideal. Only index 3 is unspanned in this set which has the two vectors (2, 0, 0) and (0, 2, 0) corresponding to it.

Another example of a totally sequential binary circuit shows that a circuit may have more than one equivalence set, and yet have no unspanned indices for one of its equivalence sets. This circuit has the equations:

$$z'_1 = \bar{z}_3 \tag{9:16}$$

$$z'_2 = \bar{z}_1(z_2 \vee z_3)$$

$$z'_3 = \bar{z}_2(z_1 \vee z_3)$$

Let the initial state u by (0, 0, 0). The sequence of C-states will then be: (0, 0, 0), (1, 0, 0), (1, 0, 1), (2, 0, 1), (2, 1, 1), (2, 1, 2), (3, 1, 2), (3, 2, 2) etc. The initial state forms its own equivalence set, while the remaining six

states which follow it form another equivalence set having the corresponding cycling vector (2, 2, 2). Hence, no indices are unspanned.

10. Distributive Circuits

10.1 In sections 5.3 and 5.4 it was pointed out that in some cases design and synthesis of circuits could be simplified by placing more restrictions upon them. Thus, semi-modular circuits are easier to treat than more general speed independent circuits, and totally sequential circuits exhibit still fewer peculiarities of behavior. Yet, as was shown in 5.4, totally sequential circuits are unsatisfactory for those applications in which parallel action is required, so that the less restrictive concept of semi-modularity was used in the later analysis.

In this section we shall place a further restriction upon our circuits in order to simplify the problem of synthesis, but this restriction will not be so severe as to eliminate the possibility of parallel action within the circuit. This restriction is that the circuit shall be distributive.

10.2 The concept of distributive circuits is related to that of a distributive lattice in the same way that the concept of a semi-modular circuit is related to that of a semi-modular lattice. We begin with the weaker restriction, however, that C[u] be modular.

(10:1) The semi-modular lattice C[u] is said to be modular if for every three C-states $\underline{a}$, $\underline{x}$ and $\underline{y}$ in C[u], such that $\underline{a}$ covers $\underline{x}$ and $\underline{y}$ and $\underline{x} \neq \underline{y}$, we have $\underline{x}$ and $\underline{y}$ covering $\underline{x} \quad \underline{y}$.

This restriction combined with its dual (7:14) correspond to the usual definition of modularity. (See Ref. 3, page 66.) In the theory of general lattices modularity is less restrictive than distributivity, but the lattice C[u] has special properties which make these restrictions equivalent. This fact is demonstrated in the next two theorems.

(10:2) If $\underline{p}$ and $\underline{q}$ are any two C-states in C[u], and C[u] is modular, then $\underline{p} \cap \underline{q} = \underline{p} \wedge \underline{q}$.

<u>Proof</u>: Form two covering sequences in C[u]:

$\underline{a}(r, 0), \underline{a}(r, 1), \ldots, \underline{a}(r, s)$ and

$\underline{a}(0, s), \underline{a}(1, s), \ldots, \underline{a}(r, s)$,

where we take $\underline{p} = \underline{a}(r, 0)$, $\underline{q} = \underline{a}(0, s)$ and $\underline{p} \cup \underline{q} = a(r, s)$. As we have seen previously, we may construct such sequences because $\underline{p} \mathfrak{J} \underline{p} \cup \underline{q}$ and $\underline{q} \mathfrak{J} \underline{p} \cup \underline{q}$. The integers r and s are finite, and each is greater than or equal to zero.

Define $\underline{a}(i, j)$ recursively by the formula

$$\underline{a}(i, j) = \underline{a}(i, j + 1) \cap \underline{a}(i + 1, j)$$

for $0 \leq i < r$ and $0 \leq j < s$, starting with $i = r - 1$, $j = s - 1$ and proceeding to all other indices. Using induction with (10:1), we see that $\underline{a}(i, j)$ will be covered by $\underline{a}(i, j + 1)$ and by $\underline{a}(i + 1, j)$ for $0 \leq i < r$ and $0 \leq j < s$, provided we can show that $\underline{a}(i + 1, j) \neq \underline{a}(i, j + 1)$. But we may use induction to infer that $\underline{a}(i + 1, j) \neq \underline{a}(i + 1, j + 1)$ and $\underline{a}(i, j + 1) \neq \underline{a}(i + 1, j + 1)$ so that $\underline{a}(i + 1, j) \neq \underline{a}(i, j + 1)$.

It was pointed out in the proof of (7:C) that the "covers" relationship implies the $\mathcal{R}$ relationship so that we may use (7:13) to get $\underline{a}(i, j) = \underline{a}(i, j + 1) \wedge \underline{a}(i + 1, j)$ for $i = 0, 1, \ldots, r - 1$ and $j = 0, 1, \ldots, s - 1$. By induction we may replace this with the formula $\underline{a}(i, j) = \underline{a}(i, s) \wedge \underline{a}(r, j)$, since it holds for either $i = r$ or $j = s$ and if we assume it for $\underline{a}(i, j + 1)$ and $\underline{a}(i + 1, j)$ we obtain

$$\underline{a}(i, j) = \underline{a}(i, s) \wedge a(r, j + 1) \wedge \underline{a}(i + 1, s) \wedge \underline{a}(r, j) = \underline{a}(i, s) \wedge \underline{a}(r, j).$$

In the case $i = j = 0$ this formula becomes $\underline{a}(0, 0) = \underline{a}(0, s) \wedge \underline{a}(r, 0) = \underline{p} \wedge \underline{q}$. Thus $\underline{p} \wedge \underline{q}$ is a C-state and by (7:4) is equal to $\underline{p} \cap \underline{q}$.

The statement of (10:2) is the dual of (7:5) and permits us to use the symbols $\wedge$ and $\cap$ interchangeably.

(10:A) If C[u] is modular it is distributive.

Proof: We verify that the distributive laws

$$\underline{a} \cap (\underline{b} \cup \underline{c}) = (\underline{a} \cap \underline{b}) \cup (\underline{a} \cap \underline{c})$$

$$\underline{a} \cup (\underline{b} \cap \underline{c}) = (\underline{a} \cup \underline{b}) \cap (\underline{a} \cup \underline{c})$$

hold for numerical vectors if the operations $\wedge$ and $\vee$ are substituted for $\cap$ and $\cup$.

A complete equivalence between the three conditions has thus been established since it is a well known lattice theoretical result that distributivity implies modularity. (See Ref. 3, p. 134.)

(10:3) A circuit is defined as distributive with respect to an initial state u if C[u] is a distributive lattice.

Our discussion of distributive circuits will also require a further property of C[u].

(10:4) C[u] satisfies the descending chain condition.

Proof: The descending chain condition (see Ref. 3, p. 37) requires that all descending chains be finite. A descending chain in this case is a sequence of C-states $\underline{a}(1)$, $\underline{a}(2)$, ..., $\underline{a}(i)$, ..., such that $\underline{a}(i + 1) \mathcal{F} \underline{a}(i)$ and $\underline{a}(i + 1) \neq \underline{a}(i)$ for i = 1, 2, ... Since we are dealing with vectors whose components are non-negative integers, and since these vectors satisfy (7:4) we infer (10:4) immediately. C[u] need not be distributive for (10:4).

10.2 A synthesis technique, which will be developed later, depends upon the properties of the join-irreducible elements of C[u].

(10:5) The notation J[u] will be used to denote the set of join-irreducible elements of C[u]. A C-state, $\underline{a}$, is join-irreducible if $\underline{a} = \underline{x} \cup \underline{y}$ implies either $\underline{a} = \underline{x}$ or $\underline{a} = \underline{y}$. (See Ref. 3, p. 20.)

It has been shown by G. Birkhoff that each element in a distributive lattice satisfying the descending chain condition has a unique representation as an

irredundant join of join-irreducible elements, and that therefore there is a one-to-one correspondence between distributive lattices L satisfying the descending chain condition and partially ordered sets p satisfying the descending chain condition, in which p is isomorphic to the subset of join-irreducible elements of L. (See Ref. 3, p. 142-3.) From these theorems we may state:

(10:6) If C[u] is distributive, each C-state may be represented as a unique irredundant join of elements of J[u].

An irredundant join is one from which no term may be removed without changing its value.

(10:7) If C[u] is distributive the set of numerical vectors of the corresponding J[u] determine the vectors of C[u] uniquely.

The importance of these results will appear in the later development of a synthesis technique which begins with the partially ordered set J[u] and makes use of (10:6) and (10:7) to construct the distributive lattice C[u].

10.3 The join-irreducible elements of C[u] may be related to the C-signals in the following way.

(10:8) In a distributive C[u] the set of non-zero join-irreducible elements is isomorphic with the set of C-signals (α, i) having $\alpha > 0$. Under this isomorphism, if (α, i) and (β, j) correspond to <u>a</u> and <u>b</u> respectively in J[u], then $\underline{a} \mathfrak{J} \underline{b}$ if and only if $(\alpha - 1, i) \subseteq (\beta - 1, j)$.

<u>Proof</u>: Let (α, i) be any C-signal. The set of all C-states inducing (α, i) must have at least one minimum C-state, since if <u>x</u> induces (α, i) there cannot be more than a finite number of C-states preceding <u>x</u> which induce (α, i). Also, there cannot be more than one minimum C-state, for if <u>a</u> and <u>b</u> are two minima, then by (10:2), $\underline{a} \cap \underline{b}$ also induces (α, i), and hence $\underline{a} \cap \underline{b} = \underline{a} = \underline{b}$. Thus <u>a</u> is unique.

The minimum C-state <u>a</u> which induces (α, i) is join-irreducible, for if $\underline{a} = \underline{x} \cup \underline{y}$, then either <u>x</u> induces (α, i) or <u>y</u> induces (α, i) by (7:5) so either $\underline{a} = \underline{x}$ or $\underline{a} = \underline{y}$. This means that each (α, i) determines a unique join-irreducible C-state <u>a</u>, which is the minimum C-state inducing (α, i).

Now, let $\underline{b}$ be any join-irreducible C-state. We construct all C-signals induced by $\underline{b}$. They are $(\beta_1, 1)$, $(\beta_2, 2)$, ..., (β_n, n), where $\beta_j = \underline{b}_j$ for $j = 1, 2, \ldots, n$. Let $\underline{c}(1)$, $\underline{c}(2)$, ..., $\underline{c}(n)$ be the join-irreducible C-states corresponding to these C-signals. Then, by construction, $\underline{c}(j) \mathfrak{J} \underline{b}$ for each $j = 1, 2, \ldots, n$, so $\underline{b} = \underline{c}(1) \cup \underline{c}(2) \cup \ldots \cup \underline{c}(n)$. But $\underline{b}$ is join-irreducible, so that there is at least one $\underline{c}(j)$ such that $\underline{b} = \underline{c}(j)$. This shows that there is at least one C-signal corresponding to any join-irreducible element $\underline{b}$. We now wish to show that if $\underline{b} \neq 0$ this correspondence is one-to-one.

If $\alpha = 0$ in the C-signal (α, i) then $\underline{0}$ induces (α, i), and is clearly minimal. Thus all C-signals of the form $(0, i)$ have $\underline{0}$ for their corresponding join-irreducible C-state. Now take $\alpha > 0$ in (α, i) and let $\underline{a}$ be the corresponding join-irreducible element, as before. Let $\underline{0}$, $\underline{a}(1)$, $\underline{a}(2)$, ..., $\underline{a}(r)$, $\underline{a}$ be a covering sequence in C[u] from $\underline{0}$ to $\underline{a}$. This sequence has at least two members because $\underline{a} \neq 0$. Since $\underline{a}(r)$ is covered by $\underline{a}$ it differs from $\underline{a}$ in just one component, by one, according to (7:D). Thus $\underline{a}_j(r) + 1 = \underline{a}_j$ for just one index j, and $\underline{a}_k(r) = \underline{a}_k$ for all other indices k. But, j must equal i, for otherwise $\underline{a}(r)$ would induce (α, i), which is impossible because $\underline{a}$ is the minimum C-state inducing (α, i). Thus, i is uniquely j and α is uniquely $\underline{a}_i$. This means that (α, i) is uniquely determined, and hence the mapping is one-to-one.

To demonstrate the second part of the theorem we require the lemma.

(10:8) If C[u] is distributive and $\underline{a}$ is the join-irreducible element corresponding to (α, i), then for any $\underline{x}$ either $\underline{a} \mathfrak{J} \underline{x}$ or else $\underline{x}$ is in $(\alpha - 1, i)$.

We begin by noting that if $\alpha > 0$, then $(\alpha - 1, i)$ exists. This may be seen by considering a covering sequence from $\underline{0}$ to $\underline{a}$. By (7:D) some C-state in this sequence must induce $(\alpha - 1, i)$.

If x is not in $(\alpha - 1, i)$ then $a \cap x$ induces (α, i) by (10:2). By construction of a we have $a \mathfrak{I} a \cap x$ so $a \mathfrak{I} x$. Conversely if $a \mathfrak{I} x$ then $a \cap x = a$ is not in $(\alpha - 1, i)$ so x is not in $(\alpha - 1, i)$.

Let (α, i) and (β, j) correspond to the join-irreducible elements a and b respectively. Assume $a \mathfrak{I} b$. If x is any C-state in $(\alpha - 1, i)$, we cannot have $b \mathfrak{I} x$ for otherwise $a \mathfrak{I} x$, which is impossible by (10:8). Hence x is in $(\beta - 1, j)$ by (10:8). Since x was arbitrary we have $(\alpha - 1, i) \subseteq (\beta - 1, j)$.

Next assume $(\alpha - 1, i) \subseteq (\beta - 1, j)$. Since b is not in $(\beta - 1, j)$, it cannot be in $(\alpha - 1, i)$ and hence $a \mathfrak{I} b$ by (10:8).

This completes the proof of (10:B) which, it should be noted, depends on (7:D) and, therefore, upon the assumption that the signals are independent.

(10:9) If two distributive lattices of C-states C[u] and C*[u*] determine identical partially ordered sets of C-signals, then C[u] and C*[u*] are identical.

<u>Proof</u>: Let us assume that C[u] and C*[u*] are not identical. By (10:7) we see that their corresponding sets J[u] and J*[u*] of join-irreducible elements are not identical. Hence there is at least one join-irreducible element a in J[u] which differs from the corresponding element a^* in J*[u*] but both correspond to C-signals having the same designation, say (α, i). Note that a and a^* may not be the zero elements in J[u] and J*[u*], since then they would be equal. Since $a_i = \alpha$ and $a^*_i = \alpha$, they must differ in some other component, say $a_j \neq a^*_j$. No loss of generality results from assuming $a_j < a^*_j$. Thus the C-signal (β, j) with $a^*_j = \beta > 0$ exists. Let b be the corresponding join-irreducible element in J[u]. Then a is in $(\beta - 1, j)$ so $b \not\mathfrak{I} a$ by (10:8) but a^* is not in $(\beta - 1, j)$ and $b^* \mathfrak{I} a^*$. However, J[u] and J*[u*] are isomorphic by (10:B) giving a contradiction.

10.4 We shall take the set of C-signals and their ordering relationships as the starting point for the synthesis procedure. It will be assumed, therefore,

that some verbal description of the behavior of the circuit leads to a specification of this partially ordered set. In effect, we are specifying the signal changes which occur at points within the circuit and causation relations between these changes. Naturally, not every such specification will lead to a realizable circuit, but the theorems which follow will give us restrictions on the functions (2:1c). If these restrictions are internally consistent then any set of functions which satisfies them will represent a distributive (and hence speed independent) circuit which behaves in the specified way.

There are two reasons for using the set of C-signals rather than the lattice C[u] as our starting point. In the first place, the set of C-signals is not as numerous as the set of C-states, if parallel action takes place in the circuit. In fact, if r parallel changes occur in a binary circuit, we obtain r corresponding C-signals and 2^r C-states. Secondly, the C-signals are not subject to as many restrictions as the C-states, since the C-states must form a distributive (or at least semi-modular) lattice while the C-signals merely need to be partially ordered, although in either case we must be able to obtain a consistent set of restrictions on the functions (2:1c).

(10:10) If $\underline{a}$ induces (α, i) and (γ, j), and $\underline{b}$ is the join-irreducible C-state corresponding to $(\alpha + 1, i)$, then $\underline{a}_j < \underline{b}_j$ if and only if $(\gamma, j) \subseteq (\alpha, i)$.

Proof: Assume $\underline{a}_j < \underline{b}_j$. If $\underline{x}$ is any C-state not in (α, i) we have $\underline{b} \not\geq \underline{x}$ by (10:8). Hence $\gamma < \underline{b}_j \leq \underline{x}_j$, and $\underline{x}$ is not in (γ, j).

Next assume $(\gamma, j) \subseteq (\alpha, i)$. Since $\underline{b}$ is not in (α, i) it is not in (γ, j) and we have $\underline{a}_j = \gamma < \underline{b}_j$.

(10:C) If n is greater than one and $\underline{a}$ induces (α, i), then $\underline{a}_i = \underline{a}_i'$ if and only if there is a C-signal (γ, j) induced by $\underline{a}$ such that $(\gamma, j) \subseteq (\alpha, i)$ and $j \neq i$.

Proof: Assume that such a C-signal (γ , j) exists and yet that $\underline{a}_i \neq \underline{a}_i'$. Then by (7:E) we may construct a C-state $\underline{b}$ with $\underline{b}_i = \underline{a}_i + 1$ and $\underline{b}_j = \underline{a}_j$. Thus $\underline{b}$ is in (γ , j) and not in (α , i) and we cannot have (γ , j) $\subseteq$ (α, i). Therefore $\underline{a}_i = \underline{a}_i'$.

Assume next that $\underline{a}_i = \underline{a}_i'$. If no C-signal (β , i) exists with $\beta > \alpha$ we see that (α , i) = C[u] and hence (γ, j) $\subseteq$ (α, i) for every (γ , j). If (β, i) does exist and is induced by some C-state $\underline{c}$, we may form a covering sequence from $\underline{a}$ to $\underline{a} \cup \underline{c}$ and by (7:D) obtain a C-state inducing (α + 1, i). Let $\underline{d}$ be the join-irreducible element corresponding to (α + 1, i). Assume that $\underline{a}_j \geq \underline{d}_j$ for all j $\neq$ i. Then if we form $\underline{e} = \underline{a} \cup \underline{d}$ we see that $\underline{e}_j = \underline{a}_j$ for all j $\neq$ i and $\underline{e}_i = \underline{a}_i + 1$. Hence $\underline{e}$ covers $\underline{a}$, so $\underline{a}\, \mathcal{R}\, \underline{e}$ and $\underline{e}_i \leq \underline{a}_i'$. This would mean $\underline{a}_i \neq \underline{a}_i'$ and hence we infer $\underline{a}_j < \underline{d}_j$ for some j $\neq$ i. Therefore (γ , j) $\subseteq$ (α , i) by (10:10), for some (γ, j) induced by $\underline{a}$.

(10:D) Any vector $\underline{a}$ which, when regarded as a C-state, induces only existing C-signals, and does not violate any inclusion relations among the C-signals, does represent a member of C[u].

Proof: Since $\underline{a}$, regarded as a C-state induces only existing C signals we may attempt to write it as a join of the join-irreducible elements corresponding to these C-signals. Let this join be $\underline{a}^* = \underline{b}(1) \cup \underline{b}(2) \cup \ \ldots\ \cup \underline{b}(n)$. Let us assume $\underline{a}^* \neq \underline{a}$ so that $\underline{a}_i^* \neq \underline{a}_i$ for at least one i. Then there must be some $\underline{b}(j)$ such that $\underline{b}_i(j) > \underline{b}_i(i)$. Let $\underline{b}(i)$ induce (α , i) and $\underline{b}(j)$ induce (β, j). By the argument of the previous proof we have (α , i) $\subseteq$ (β - 1, j). But this inclusion, relation is violated by the assumption that $\underline{a}$ is in (α , i) but not in (β - 1, j). Hence $\underline{a}^* = \underline{a}$ and $\underline{a}$ is in C[u].

Theorems (10:C) and (10:D) may be used to obtain a synthesis method for binary circuits. A detailed presentation of this technique will appear in a future publication dealing with synthesis.

In a binary circuit the terminal state a of any C-state $\underline{a}$ is obtainable by summing u and $\underline{a}$, and taking the residues of the components modulo 2. Also, in the binary case, we see that $a_i \neq a_i'$ implies a_i' equals the complement of a_i. Thus we are able to determine explicitly whether $a_i' = a_i$ or $a_i' = \overline{a_i}$ from (10:C) with a knowledge of the ordering relations among the C-signals, provided we know what the other signals may be. But the other signals are limited only by the limitations described in (10:D). Thus, for each signal a_i we obtain a set of restrictions on the function f_i. If all these restrictions to all f_i are applied, we obtain a set of conditions which, if consistent, are necessary and sufficient to cause the circuit to behave in a way described by the lattice C[u].

Bibliography

1. D. A. Huffman, "The Synthesis of Sequential Switching Circuits", Journal of the Franklin Institute, Vol. 257, Nos. 3 and 4 (1954).

2. G. H. Mealy, "A Method for Synthesizing Sequential Circuits", Bell Systems Technical Journal, September 1955, p.p. 1045-79.

3. G. Birkhoff, "Lattice Theory", American Mathematical Society Colloquim Publications, Vol. 25, (1948).